

MENU

SEARCH

INDEX

DETAIL

PATENT

1 / 1

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-030613

(43)Date of publication of application : 31.01.2003

(51)Int.Cl.

G06K 19/073

G06K 17/00

G11C 16/02

(21)Application number : 2001-213036

(71)Applicant : HITACHI LTD

(22)Date of filing : 13.07.2001

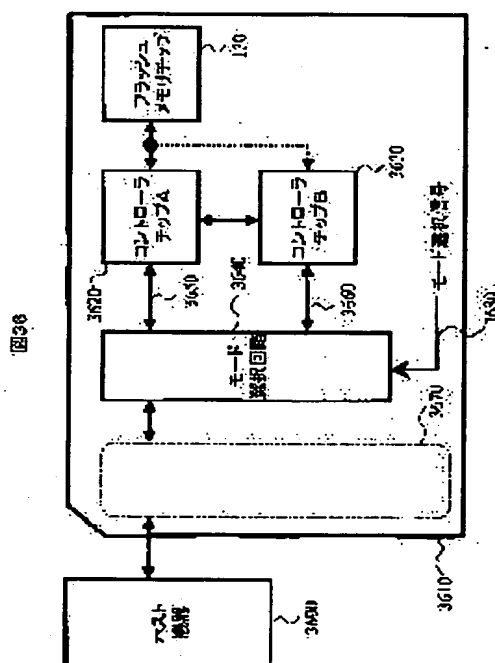
(72)Inventor : TSUNODA MOTOYASU  
MIZUSHIMA EIGA  
KATAYAMA KUNIHIRO

(54) STORAGE DEVICE AND DATA PROCESSOR PROVIDED WITH THE STORAGE DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To improve the handleability of a card type storage device.

SOLUTION: The card type storage device 3610 is provided with a plurality of controller chips (3620 and 3630) and provided with a means supporting interface modes corresponding to the respective chips and switching and discriminating the mode by mode selection signals 3680.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-30613

(P2003-30613A)

(43) 公開日 平成15年1月31日(2003.1.31)

(51) Int.Cl.<sup>7</sup>

識別記号

F I

テーマコード(参考)

G 0 6 K 19/073

G 0 6 K 17/00

S 5 B 0 2 5

17/00

19/00

P 5 B 0 3 5

G 1 1 C 16/02

G 1 1 C 17/00

6 0 1 P 5 B 0 5 8

6 0 1 E

審査請求 未請求 請求項の数7 O L (全 32 頁)

(21) 出願番号 特願2001-213036(P2001-213036)

(22) 出願日 平成13年7月13日(2001.7.13)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 角田 元泰

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 水島 永雅

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74) 代理人 100075096

弁理士 作田 康夫

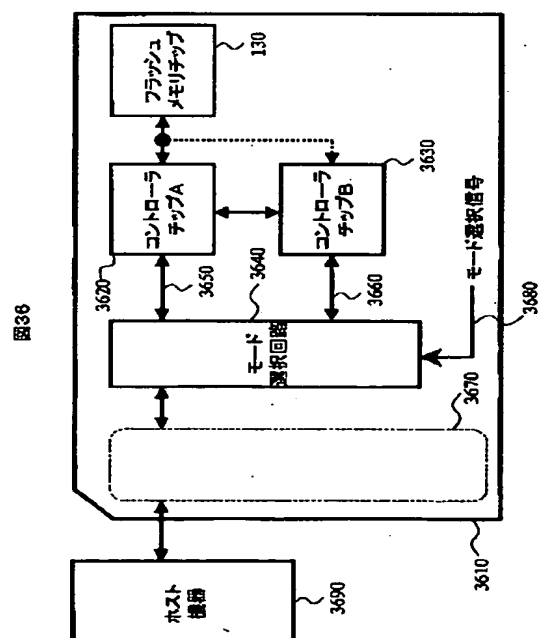
最終頁に続く

(54) 【発明の名称】 記憶装置及び記憶装置を備えたデータ処理装置

## (57) 【要約】

【課題】本発明は、カード型記憶装置の使い勝手を向上することを目的とする。

【解決手段】本発明は、カード型記憶装置3610において、複数のコントローラチップ(3620、3630)を備え、各々のチップに対応したインターフェースモードをサポートし、モードの切り替え及び判別をモード選択信号3680によって行う手段とを備える。



## 【特許請求の範囲】

【請求項1】 ホスト機器と接続される外部端子と、少なくとも2つのインターフェースモードを制御する制御手段と、前記少なくとも2つのインターフェースモードから1つのインターフェースモードを選択する選択手段と、前記選択手段による選択結果に基づき、選択された前記インターフェースモードで前記外部端子を制御する外部端子制御手段とを有することを特徴とする記憶装置。

【請求項2】 前記制御手段は、前記少なくとも2つのインターフェースモードのうち、第1のインターフェースモードを制御するコントローラチップと、第2のインターフェースモードを制御するコントローラチップとを有し、前記外部端子制御手段は、前記選択されたインターフェースモードを制御するコントローラチップの外部入出力信号と前記外部端子とを接続する手段とを備えることを特徴とする請求項1記載の記憶装置。

【請求項3】 記憶装置に記憶されたデータを用いてデータの処理を行うデータ処理装置において、前記記憶装置を制御する制御手段と、前記記憶装置が挿入されるソケットと、前記ソケット及び前記制御手段と接続される、インターフェースモードを検出する検出手段と、前記検出手段による検出結果がICカードモードの場合に、前記ソケットと前記制御手段の信号線とを接続する手段とを有することを特徴とするデータ処理装置。

【請求項4】 前記ソケットは、前記記憶装置が挿入されたことを検出する第1のスイッチと、前記第1のスイッチによって反応する第2のスイッチを有し、前記第2のスイッチによって前記記憶装置におけるインターフェースモードのサポート状態を検出するサポート検出手段と、前記サポート検出手段の検出結果に基づき、前記記憶装置のインターフェースモードを判定する手段とを有することを特徴とする請求項3記載のデータ処理装置。

【請求項5】 ホスト機器が有するスイッチに応答する第3のスイッチを有し、前記第3のスイッチの状態によりインターフェースモードを選択する選択手段と、前記選択手段によって選択されたインターフェースモードで前記外部端子を制御する手段とを有することを特徴とする請求項1記載の記憶装置。

【請求項6】 該記憶装置は、カード型記憶装置であって、カード同一辺上の両端に誤挿入防止のための第1の切り込み及び第2の切り込みを有し、前記第1の切り込みによって第1のインターフェースモードを一義的に決定するための手段と、前記第2の切り込みによって第2のインターフェースモードを一義的に決定するための手段とを有することを特徴とする請求項1記載の記憶装置。

【請求項7】 カード型記憶装置に記憶されたデータを用いてデータの処理を行うデータ処理装置において、第4のスイッチと、前記第4のスイッチの状態に応じて、第

1のインターフェースモードまたは第2のインターフェースモードを選択する選択手段と、前記選択手段によって選択されたインターフェースモードに基づきデータを処理する手段とを有することを特徴とするデータ処理装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、セキュリティ機能を有する記憶装置、その記憶装置が挿入可能なホスト機器、及びその記憶装置が挿入されたホスト機器に係り、特に、フラッシュメモリチップ及びコントローラを有するメモリカード、そのメモリカードが挿入可能な装置、並びにそのメモリカードが挿入された端末装置に関する。

## 【0002】

【従来の技術】 ICカードは、プラスチックカード基板中にIC（集積回路）チップを埋め込んだものであり、その表面にICチップの外部端子を持つ。ICチップの外部端子には電源端子、クロック端子、データ入出力端子などがある。ICチップは、接続装置が外部端子から電源や駆動クロックを直接供給することによって動作する。ICカードは、外部端子を通して端末機などの接続装置との間で電気信号を送受信することにより、接続装置と情報交換をおこなう。情報交換の結果として、ICカードは計算結果や記憶情報の送出、記憶情報の変更をおこなう。ICカードは、これらの動作仕様に基づいて、機密データ保護や個人認証などのセキュリティ処理を実行する機能を持つことができる。ICカードは、クレジット決済やバンキングなど機密情報のセキュリティが必要とされるシステムにおいて、個人識別のためのユーザデバイスとして利用されている。

## 【0003】

【発明が解決しようとする課題】 セキュリティシステムにおいて利用されるICカードは、秘密情報を用いて演算を行う際に、その秘密情報あるいはその秘密情報を推定できるような情報をICカードの外部にももらさないように設計される必要がある。すなわち、耐タンパ性を持つことが必要とされる。このようなICカードの外部にもらしてはならない秘密情報を解析する攻撃方法としては、タイミング解析、電力差分析、故障利用解析などが知られている。

【0004】 タイミング解析は、暗号処理時間が秘密情報の内容に依存して異なる場合、その時間差を統計的に解析して秘密情報を推定する攻撃法である。暗号アルゴリズムを実装する際、処理時間の短縮やプログラムサイズの縮小を目的として、秘密情報の内容に依存して不要処理をスキップしたり分岐処理を行ったりするような最適化を適用することがある。このような最適化を適用すると、暗号処理時間が秘密情報の内容に依存して異なる。そのため処理時間を見ることで秘密情報の内容を推

定できる可能性がある。

【0005】電力差分析は、暗号処理の実行中にICカードの電源端子から供給される電力を測定し、そこから消費電力の差分を解析することにより秘密情報を推定する攻撃法である。

【0006】故障利用解析は、ICカードの計算誤りを利用した攻撃法である。ICカードに一過性の故障あるいは他の機能に影響を与えない範囲の限定的な障害を与え、ICカードに攻撃者の望む異常な処理を行わせる。ICカードに高電圧を加えたり、瞬間的にクロック周波数や駆動電圧を変動させることにより故意にエラーを発生させた場合、その結果得られる誤った計算結果と正しい計算結果から秘密情報が得られる可能性がある。

【0007】ICカードは、実用上、これらの攻撃法に対する対策手段を持たなければならない。

【0008】本発明の目的は、セキュリティを向上した記憶装置を提供することである。

【0009】また、ICカードはクレジットカードサイズの形状のものが主流であるが、小型の携帯端末で用いる場合は大きく使い勝手が悪い。本発明の他の目的は、ICカードの使い勝手を向上した記憶装置を提供することにある。

【0010】

【課題を解決するための手段】上記課題を解決するため、本発明は、データを記憶するための記憶装置において、ホストと通信するための外部端子と、少なくとも2系統のホストインタフェースを制御する手段と、インタフェースを選択する手段と、該選択結果に基づき、選択されたインタフェースを該外部端子に接続する手段とを備える。

【0011】上記、少なくとも2系統のホストインタフェースは、ホストインタフェースを制御する少なくとも2系統のコントローラチップにより制御され、該選択されたホストインタフェースを制御するコントローラチップの外部入出力信号と該外部端子を接続する手段とを備える。

【0012】又は、本発明は、ICカードに記憶されたデータを用いて処理するデータ処理装置において、ICカードを制御する手段と、該記憶装置を挿入するためのソケットと、該ソケットと該制御手段との中間に配置され、インターフェースモードを検出する手段と、該検出結果がICカードモードの場合において該ソケットと該制御手段の信号線を接続する手段とを備える。

【0013】上記、該ソケットは、該記憶装置が挿入されたことを検出する第1のスイッチと、第1のスイッチによって反応する第2のスイッチを具備し、第2のスイッチによって該記憶装置におけるインターフェースモードのサポート状態を検出する手段と、該検出結果に基づき、ICカードモードを判定する手段とを備える。

【0014】また、該記憶装置は、該第2のスイッチに

よって反応し、インターフェースモードを選択する第3のスイッチを有し、該第3のスイッチの状態によりインタフェースを選択し、選択されたインタフェースを該外部端子に接続する手段とを備える。

05 【0015】又は、本発明は、データを記憶するためのカード型記憶装置において、カード同一辺上の両端に誤挿入防止のための第1の切り込みと第2の切り込みを具備し、該第1の切り込みによって第1のインタフェースを一義的に決定するための手段と、該第2の切り込みによって第2のインタフェースを一義的に決定するための手段とを備える。また、該カード型記憶装置に記憶されたデータを用いて処理するデータ処理装置において、第4のスイッチを具備し、該記憶装置を挿入した場合において、該第4のスイッチにより、第1のインタフェース  
10 または第2のインタフェースを選択する手段と、該選択されたインタフェースに基づきデータを処理する手段とを備える。

【0016】

【発明の実施の形態】図22は、本発明を適用したMultiMediaCard (MultiMediaCardはInfineon Technologies AGの登録商標である。以下、「MMC」と略記する。)の内部構成を簡単に表した図である。MMC110は、MultiMediaCard仕様に準拠するのが好ましい。  
20 MMC110は、外部に接続したホスト機器220がMultiMediaCard仕様に準拠したメモリカードコマンドを発行することによって、機密データ保護や個人認証などに必要な暗号演算をおこなうセキュリティ処理機能を持つ。ホスト機器220は、例えば、携帯電話、携帯情報端末(PDA)、パーソナルコンピュータ、音楽再生(及び録音)装置、カメラ、ビデオカメラ、自動預金預払器、街角端末、決済端末等が該当する。

【0017】MMC110は、MMC外部端子140、コントローラチップ120、フラッシュメモリチップ130、ICカードチップ150を持つ。フラッシュメモリチップ130は、不揮発性の半導体メモリを記憶媒体とするメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。MMC外部端子140は7つの端子から構成され、外部のホスト機器220と情報交換するために、電源供給端子、クロック入力端子、コマンド入出力端子、データ入出力端子、グランド端子を含む。コントローラチップ120は、MMC110内部の他の構成要素(MMC外部端子140、フラッシュメモリチップ130、ICカードチップ150)と接続されており、これらを制御するマイコンチップである。ICカードチップ150は、ICカードのプラスチック基板中に埋め込むためのマイコンチップであり、その外部端子、電気信号プロトコル、コマンドはISO/  
35 IEC7816規格に準拠している。ICカードチップ  
40  
45  
50

150の外部端子には、電源供給端子、クロック入力端子、リセット入力端子、I/O入出力端子、グランド端子がある。コントローラチップ120は、ICカードチップ150の外部端子からICカードチップ150にICカードコマンドを発行することによって、外部のホスト機器220から要求されたセキュリティ処理に必要な演算をおこなう。

【0018】図26は、本発明のICカードチップの内部構成を示す図である。ICカードチップ150は、演算処理を行うためのCPU（マイコン）158と、データ（プログラムを含む。）を記憶するためのROM（Read Only Memory）159とRAM（Random Access Memory）160とEEPROM（Electrically Erasable Programmable ROM）162と、暗号／復号に間する処理を行うための暗号コプロセッサ163と、外部とデータを送受信するためのシリアルインターフェース161とを備え、それらは、バス164によって接続される。そして、その暗号コプロセッサ163によって、ホスト機器220からのコマンドに応じて、ICカードチップ150自らが、セキュリティ処理を実行することが可能である。尚、暗号コプロセッサ163（ハードウェア）の代わりに、プログラム（ソフトウェア）に従ってCPU158がセキュリティ処理を実行してもよい。

【0019】一方、フラッシュメモリチップ130は、記憶素子を備えるが、マイコンは存在しない。セキュリティ処理は、例えば、ICカードチップ150内の記憶領域にデータが書き込まれるとき、又は、ICカードチップ150内の記憶領域からデータが読み出されるときに実行される。ICカードチップ150のEEPROMの記憶容量は、フラッシュメモリチップ130の記憶容量より小さい。但し、ICカードチップ150のEEPROMの記憶容量は、フラッシュメモリチップ130の記憶容量と同じでもよいし、大きくてもよい。

【0020】ICカードチップ150には、セキュリティ評価基準の国際標準であるISO/IEC15408の評価・認証機関によって認証済みである製品を利用する。一般に、セキュリティ処理をおこなう機能を持つICカードを実際の電子決済サービスなどで利用する場合、そのICカードはISO/IEC15408の評価・認証機関による評価と認定を受ける必要がある。MMCにセキュリティ処理をおこなう機能を追加することによってMMC110を実現し、それを実際の電子決済サービスなどで利用する場合、MMC110も同様にISO/IEC15408の評価・認証機関による評価と認定を受ける必要がある。本発明によれば、MMC110は、評価・認証機関によって認証済みのICカードチップ150を内蔵し、そのICカードチップ150を利用してセキュリティ処理をおこなう構造を持つことにより、セキュリティ処理機能を得る。したがって、MMC110はISO/IEC15408に基づくセキュリテ

ィ評価基準を容易に満足することができ、MMCにセキュリティ処理機能を追加するための開発期間を短縮することができる。

【0021】MMC110は、MultiMediaCard仕様に準拠した外部インタフェースを持つのが好ましい。MMC110は、一種類の外部インタフェースを通じて、標準メモリカードコマンド（フラッシュメモリチップ130へアクセスするためのコマンド）に加えて、セキュリティ処理を実行するコマンドを受け付ける必要がある。コントローラチップ120は、MMC110が受信したコマンドが標準メモリカードコマンドであるか、セキュリティ処理を実行するコマンドであるかによって、アクセスすべきチップを選択し、コマンド処理を分配する機能を持つ。本発明によれば、標準メモリカードコマンドを受信したならば、フラッシュメモリチップ130を選択し、これにフラッシュメモリコマンドを発行してホストデータを読み書きできる。また、セキュリティ処理を実行するコマンドを受信したならば、ICカードチップ150を選択し、これにICカードコマンドを発行してセキュリティ処理を実行することができる。

【0022】ICカードチップ150の外部端子は、グランド端子を除いて、電源供給端子、クロック入力端子、リセット入力端子、I/O入出力端子がコントローラチップ120に接続されている。

【0023】コントローラチップ120は、電源供給端子、クロック入力端子を通して、ICカードチップ150への電源供給、クロック供給を制御する。本発明によれば、ホスト機器220からセキュリティ処理を要求されないときには、ICカードチップ150への電源供給やクロック供給を停止させることができ、MMC110の電力消費を削減することができる。電源供給されていないICカードチップ150を、ICカードコマンドを受信できる状態にするには、まず、ICカードチップ150に電源供給を開始し、リセット処理を施すことが必要である。コントローラチップ120は、MMC110がホスト機器220からセキュリティ処理を実行するコマンドを受信したのを契機に、電源供給端子を通してICカードチップ150への電源供給を開始する機能を持つ。また、コントローラチップ120は、MMC110がホスト機器220からセキュリティ処理を実行するコマンドを受信したのを契機に、リセット入力端子を通してICカードチップ150のリセット処理をおこなう機能を持つ。本発明によれば、コントローラチップ120は、セキュリティ処理を実行するコマンドを受信するまでICカードチップ150への電源供給を停止させておくことができる。したがって、MMC110の電力消費を削減することができる。

【0024】コントローラチップ120は、ICカードチップ150のクロック入力端子を通してICカードチ

ップ150に供給するクロック信号をMMC110内部で発生し、その周波数、供給開始タイミング、供給停止タイミングを制御する機能を持つ。本発明によれば、MMC外部端子140のクロック入力端子のクロック信号と無関係にすることができるため、ホスト機器220によるタイミング解析、電力差分析、故障利用解析と呼ばれる攻撃法に対してセキュリティが向上する。

【0025】図21は、フラッシュメモリチップ130の詳細な内部構成を表した図である。フラッシュメモリチップ130は、ホストデータ領域2115と管理領域2110を含む。ホストデータ領域2115は、セクタ単位に論理アドレスがマッピングされている領域であり、ホスト機器220が論理アドレスを指定してデータを読み書きできる領域である。ホストデータ領域2115は、ユーザファイル領域2130とセキュリティ処理アプリケーション領域2120を含む。ユーザファイル領域2130は、ユーザが自由にファイルデータを読み書きできる領域である。セキュリティ処理アプリケーション領域2120は、ホスト機器220がセキュリティ処理アプリケーションに必要なデータを格納する領域であり、ユーザが不正にアクセスしないように、ホスト機器220のセキュリティ処理アプリケーションが論理的にユーザアクセス制限をかける。ここに格納するデータとしては、ホスト機器220のアプリケーションプログラム、そのアプリケーション専用のデータ、セキュリティ処理に使用される証明書など（例えば、電子決済アプリケーションプログラム、電子決済ログ情報、電子決済サービス証明書など）が可能である。本発明によれば、MMC110が、ホスト機器220がセキュリティ処理をおこなう上で使用するデータをホスト機器220の代わりに格納するため、ホスト機器220にとって利便性が向上する。

【0026】一方、管理領域2110は、コントローラチップ120がICカードチップ150を管理するための情報を格納する領域である。管理領域2110は、ICカード制御パラメータ領域2111、ICカード環境設定情報領域2112、CLK2設定情報領域2113、セキュリティ処理バッファ領域2114、セキュリティ処理ステータス領域2116を含む。2111～2116の領域の詳細な使用方法については後述する。

【0027】コントローラチップ120は、フラッシュメモリチップ130の管理領域2110のセキュリティ処理バッファ領域2114を、ICカードチップ150でセキュリティ処理を実行する際のメインメモリまたはバッファメモリとして利用する。ホスト機器220がセキュリティ処理を実行するコマンドによりMMC110にアクセスした際に、MMC110がホスト機器220からICカードチップ150に一度に送信できないほどの大きなサイズのセキュリティ関連データを受信したならば、コントローラチップ120はフラッシュメモリチ

ップ130へのアクセスを選択し、そのデータを十分な容量を持つセキュリティ処理バッファ領域2114に一時的に格納する。ICカードチップ150に一度に送信できないほどのサイズは、ICカードコマンドの許容データサイズ（例えば、255バイト又は256バイト）を超えるサイズである。そして、コントローラチップ120はそれをICカードチップ150に送信できるサイズのデータに分割し、分割データをフラッシュメモリチップ130から読み出し、段階的にICカードチップ150に送信する。つまり、分割されたデータの読み出し、書き込みを繰り返す。本発明によれば、ホスト機器220にとって、大きなサイズのセキュリティ関連データを扱うことができるので、セキュリティ処理の利便性が向上する。

【0028】セキュリティ処理バッファ領域2114を含む管理領域2110は、ホスト機器220が不正にアクセスしてセキュリティ処理を解析することができないように、コントローラチップ120により物理的にホストアクセス制限がかけられている。つまり、管理領域2110はホスト機器220が直接データを読み書きできない。本発明によれば、ホスト機器220がセキュリティ処理バッファ領域2114の内容を自由に読み出したたり改ざんすることができないため、セキュリティ処理の信頼性や安全性が向上する。

【0029】図23は、MMC110を利用したセキュリティ処理の一例として、コンテンツ配信のセキュリティ処理を表したものである。コンテンツプロバイダ2310は、MMC110を所有するユーザにコンテンツ2314を販売する業者である。ホスト機器220は、この例では、コンテンツプロバイダ2310とネットワークなどを介して接続することができる端末機である。ユーザはMMC110をホスト機器220に接続してコンテンツ2314を購入する。以下、その手順を説明する。

【0030】まず、ホスト機器220はMMC110に、フラッシュメモリチップ130に格納されたユーザ証明書2321を読み出すコマンドを発行する。MMC110のコントローラチップ120は、フラッシュメモリチップ130のセキュリティ処理アプリケーション領域2120に格納されたユーザ証明書2321を読み出し、それをホスト機器220に送信する。そして、ホスト機器220はそれをコンテンツプロバイダ2310に送信する。コンテンツプロバイダ2310はユーザ証明書2321につけられたデジタル署名を検証する（2311）。検証が成功したならば、乱数発生器によりセッション鍵を生成し（2312）、それをユーザ証明書2321から抽出したユーザ公開鍵によって暗号化する（2313）。さらに、コンテンツ2314をそのセッション鍵によって暗号化する（2315）。

【0031】コンテンツプロバイダ2310はステップ

2313の結果をホスト機器220に送信する。ホスト機器220は、ステップ2313の結果をユーザ秘密鍵2322によって復号するセキュリティ処理を要求するコマンドを、MMC110に発行する。コントローラチップ120は、ステップ2313の結果をユーザ秘密鍵2322によって復号するICカードコマンドを、ICカードチップ150に発行する。ICカードチップ150は、ユーザ秘密鍵2322によってステップ2313の結果を復号して、セッション鍵を取得する(2323)。ホスト機器220は、この復号処理が成功したかを示す情報を出力させるコマンドをMMC110に発行する。コントローラチップ120は、ICカードチップ150の出力する復号結果(復号処理が成功したかを示すICカードレスポンス)をもとにしてホスト機器220の求める情報を構築する。そして、MMC110はその情報をホスト機器220に送信する。

【0032】次に、コンテンツプロバイダ2310は、ステップ2315の結果を、ホスト機器220に送信する。ホスト機器220は、ステップ2313の結果をセッション鍵(ステップ2323によって取得した鍵)によって復号するセキュリティ処理を要求するコマンドを、MMC110に発行する。コントローラチップ120は、ステップ2315の結果をセッション鍵によって復号するICカードコマンドを、ICカードチップ150に発行する。ICカードチップ150は、セッション鍵によってステップ2315の結果を復号して、コンテンツ2314を復元する(2324)。コントローラチップ120は、このコンテンツ2314をICカードチップ150から受信し、フラッシュメモリチップ130に書きこむ。ホスト機器220は、この復号処理が成功したかを示す情報を出力させるコマンドをMMC110に発行する。コントローラチップ120は、ICカードチップ150の出力する復号結果(復号処理が成功したかを示すICカードレスポンス)をもとにしてホスト機器220の求める情報を構築する。そして、MMC110はその情報をホスト機器220に送信する。ホスト機器220が、コンテンツを無事に受信したことをコンテンツプロバイダ2310に伝え、コンテンツプロバイダ2310はユーザ証明書に記載されたユーザにコンテンツ料金を課金する。

【0033】ユーザは、ホスト機器220でMMC110内のフラッシュメモリチップ130に格納されたコンテンツ2314を読み出して利用することができる。また、フラッシュメモリチップ130の記憶媒体に大容量のフラッシュメモリを使用すれば、多くのコンテンツを購入できる。本発明によれば、コンテンツ配信におけるセキュリティ処理とコンテンツ蓄積の両方をMMC110によって容易に実現できる。コンテンツ料金の決済を、ICカードチップ150を利用して行ってもよい。

【0034】図24と図25は、それぞれ、本発明をS

Dカード(幅24ミリメートル、長さ32ミリメートル、厚さ2.1ミリメートルで、9つの外部端子を持ち、フラッシュメモリを搭載した小型メモリカードである。)とメモリスティック(メモリスティックはソニー株式会社の登録商標である。)に適用したときの簡単な内部構成図を表したものである。本発明を適用したSDカード2410は、SDカードコントローラチップ2420、フラッシュメモリチップ2430、SDカード外部端子2440、ICカードチップ150を含む。本発明を適用したメモリスティック2510は、メモリスティックコントローラチップ2520、フラッシュメモリチップ2530、メモリスティック外部端子2540、ICカードチップ150を含む。フラッシュメモリチップ2430と2530は、不揮発性の半導体メモリを記憶媒体とするメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。SDカードコントローラチップ2420とメモリスティックコントローラチップ2520はそれぞれSDカードとメモリスティック内の他の構成要素を制御するマイコンチップである。

【0035】SDカード外部端子2440は9つの端子からなり、それらの位置は、端からData2端子2441、Data3端子2442、Com端子2443、Vss端子2444、Vdd端子2445、Clock端子2446、Vss端子2447、Data0端子2448、Data1端子2449の順で並んでいる。Vdd端子2445は電源供給端子、Vss端子2444と2447はグランド端子、Data0端子2448とData1端子2449とData2端子2441とData3端子2442はデータ入出力端子、Com端子2443はコマンド入出力端子、Clock端子2446はクロック入力端子である。SDカード2410は、外部に接続するSDカードホスト機器2460とのインタフェース仕様にMMC110と違いがあるものの、MMC外部端子140と非常に類似した外部端子を持ち、MMC110と同様に外部からコマンドを発行することにより動作する特徴を持つため、本発明を適用することができる。

【0036】一方、メモリスティック外部端子2540は10個の端子からなり、それらの位置は、端からGnd端子2541、BS端子2542、Vcc端子2543、予約端子Rsvを1つ飛ばしてDIO端子2544、INS端子2545、予約端子Rsvを1つ飛ばしてSCK端子2546、Vcc端子2547、Gnd端子2548の順で並んでいる。Vcc端子2543と2547は電源供給端子、Gnd端子2541と2548はグランド端子、DIO端子2544はコマンドおよびデータ入出力端子、SCK端子2546はクロック入力端子である。メモリスティック2510は、外部に接続するメモリスティックホスト機器2560とのイン

タフェース仕様にMMC110と違いがあるものの、MMC110と同様に外部からコマンドを発行することにより動作する特徴を持つため、本発明を適用することができる。

【0037】図1は、本発明を適用したMMCの詳細な内部構成図を表したものである。また、図2は、図1のMMC110と接続したホスト機器220の構成とその接続状態を表したものである。ホスト機器220は、VCC1電源221、CLK1発振器222、ホストインタフェース223を持つ。

【0038】MMC110は、外部のホスト機器220と情報交換するためのMMC外部端子140を持つ。MMC外部端子140は、CS端子141、CMD端子142、GND1端子143および146、VCC1端子144、CLK1端子145、DAT端子147の7つの端子とを含む。MultiMediaCard仕様は、MMCの動作モードとしてMMCモードとSPIモードという2種類を規定しており、動作モードによってMMC外部端子140の使用法は異なる。本実施例ではMMCモードでの動作の場合について詳細に説明する。

【0039】VCC1端子144は、VCC1電源221と接続されており、ホスト機器220がMMC110に電力を供給するための電源端子である。GND1端子143および146は、VCC1電源221と接続されており、MMC110の電氣的なグランド端子である。GND1端子143とGND1端子146は、MMC110内部で電氣的に短絡されている。CS端子141は、ホストインタフェース223に接続されており、SPIモードの動作において使用される入力端子である。ホスト機器220が、MMC110にSPIモードでアクセスするときには、CS端子141にLレベルを入力する。MMCモードの動作では、CS端子141を使用する必要はない。CMD端子142は、ホストインタフェース223に接続されており、ホスト機器220が、メモリカードインタフェース仕様に準拠したメモリカードコマンドをMMC110に送信したり、同仕様に準拠したメモリカードレスポンスをMMC110から受信するために使用する入出力端子である。

【0040】DAT端子147は、ホストインタフェース223に接続されており、ホスト機器220が、メモリカードインタフェース仕様に準拠した形式の入力データをMMC110に送信したり、同仕様に準拠した形式の出力データをMMC110から受信するために使用する入出力端子である。CLK1端子145は、CLK1発振器222に接続されており、CLK1発振器222が生成するクロック信号が入力される端子である。ホスト機器220が、CMD端子142を通してメモリカードコマンド、メモリカードレスポンスを送受信したり、DAT端子147を通してホストデータを送受信するときに、CLK1端子145にクロック信号が入力され

る。ホストインタフェース223には、CLK1発振器222からクロック信号が供給されており、メモリカードコマンド、メモリカードレスポンス、ホストデータは、CLK1発振器222が生成するクロック信号にビット単位で同期して、ホスト機器220とMMC110との間を転送される。

【0041】MMC110は、コントローラチップ120を持つ。コントローラチップ120は、CPU121、フラッシュメモリ1/F制御回路122、MMC1/F制御回路123、CLK0発振器124、VCC2生成器125、VCC2制御回路126、CLK2制御回路127、ICカード1/F制御回路128とを含む。これらの構成要素121~128は、ホスト機器220からVCC1端子144やGND1端子143、146を通して供給された電力により動作する。MMC1/F制御回路123は、CS端子141、CMD端子142、CLK1端子145、DAT端子147と接続されており、MMC110がそれらの端子を通してホスト機器220と情報交換するためのインタフェースを制御する論理回路である。CPU121は、MMC1/F制御回路123と接続されており、MMC1/F制御回路123を制御する。

【0042】MMC1/F制御回路123がCMD端子142を通してホスト機器220からメモリカードコマンドを受信すると、MMC1/F制御回路123はそのコマンドの受信が成功したかどうかの結果をホスト機器220に伝えるためCMD端子142を通してホスト機器220にレスポンスを送信する。CPU121は、受信したメモリカードコマンドを解釈し、コマンド内容に応じた処理を実行する。また、そのコマンド内容に応じてホスト機器220とDAT端子147を通してデータの送受信をおこなう必要がある場合、CPU121は、MMC1/F制御回路123へのデータの送出、MMC1/F制御回路123からのデータの取得をおこなう。さらに、CPU121は、MMC1/F制御回路123とホスト機器220との間のデータ転送手続きも制御する。例えば、ホスト機器220から受信したデータの処理中に、ホスト機器220がMMC110への電源供給を停止することがないように、CPU121はDAT端子147にLレベルを出力させ、MMC110がビジー状態であることをホスト機器220に伝える。CLK0発振器124は、CPU121と接続され、CPU121を動作させる駆動クロックを供給する。

【0043】MMC110は、フラッシュメモリチップ130を持つ。フラッシュメモリチップ130は、不揮発性の半導体メモリを記憶媒体とするメモリチップである。フラッシュメモリチップ130は、ホスト機器220からVCC1端子144やGND1端子143、146を通して供給された電力により動作する。フラッシュメモリチップ130は、外部からのフラッシュメモリコ



マンドに従って、入力されたデータを不揮発性の半導体メモリに格納するライト機能、また同メモリに格納されたデータを外部に出力するリード機能を持つ。フラッシュメモリI/F制御回路122は、フラッシュメモリチップ130にフラッシュメモリコマンドを発行したり、そのコマンドで入出力するデータを転送するための論理回路である。CPU121は、フラッシュメモリI/F制御回路122を制御し、フラッシュメモリチップ130にデータのライト機能やリード機能を実行させる。ホスト機器220から受信したデータをフラッシュメモリチップ130にライトしたり、フラッシュメモリチップ130に格納されたデータをホスト機器220に送信する必要があるとき、CPU121は、フラッシュメモリI/F制御回路122とMMC I/F制御回路123の間のデータ転送を制御する。

【0044】MMC110は、ICカードチップ150を持つ。ICカードチップ150は、ICカードの基板中に埋め込むことを目的として設計されたICチップであり、ICカードの外部端子規格に準拠した8つの外部端子を持つ。このうち6つの端子は、ICカードの外部端子規格により使用法が割り付けられており、残りの2つは将来のための予備端子である。その6つの端子は、VCC2端子151、RST端子152、CLK2端子153、GND2端子155、VPP端子156、I/O端子157である。

【0045】ICカードチップ150のグランド端子は、MMC外部端子140のGRN1（グランド端子）146に接続される。ICカードチップ150のVCC2端子（電源入力端子）151は、コントローラチップ120のVCC2制御回路126に接続される。ICカードチップ150のRST端子（リセット入力端子）152とI/O端子（データ入出力端子）157は、コントローラチップ120のICカードI/F制御回路128に接続される。ICカードチップ150のCLK2端子（クロック入力端子）153は、コントローラチップ120のCLK2制御回路127に接続される。

【0046】フラッシュメモリチップ130のVCC端子（電源入力端子）は、MMC外部端子140のVCC1144に接続される。フラッシュメモリチップ130のVSS端子（グランド端子）は、MMC外部端子140のGRD1146に接続される。フラッシュメモリチップ130のI/O端子（データ入出力端子）とレディ/ビジー端子とチップイネーブル端子とアウトプットイネーブル端子とライトイネーブル端子とクロック端子とリセット端子とは、コントローラチップ120のフラッシュメモリI/F制御回路122に接続される。

【0047】VCC2端子151は、ICカードチップ150に電力を供給するための電源端子である。VCC2制御回路126は、MOS-FET素子を用いたスイッチ回路によりVCC2端子151への電力の供給開始

と供給停止を制御する回路である。VCC2生成器125はVCC2端子151に供給する電圧を発生し、それをVCC2制御回路126に供給する。ICカードの電気信号規格はICカードの動作クラスとしてクラスAとクラスBを規定している。VCC2端子151に供給する標準電圧は、クラスAでは5V、クラスBでは3Vである。本発明はICカードチップ150の動作クラスによらず適用できるが、本実施例ではICカードチップ150がクラスBで動作する場合について詳細に説明する。VPP端子156は、ICカードチップ150がクラスAで動作する時に、内部の不揮発性メモリにデータを書き込んだり消去したりするために使用される可変電圧を供給する端子であり、クラスBで動作する時には使用しない。GND2端子155は、ICカードチップ150の電気的なグランド端子であり、GND1端子143、146と短絡されている。VCC2制御回路126はCPU121と接続され、CPU121はVCC2端子151への電力供給の開始と停止を制御することができる。ICカードチップ150を使用しないときは、CPU121はVCC2端子151への電力供給を停止することができる。MMC110は、ICカードチップ150への電力供給を停止することにより、それが消費する電力を節約することができる。ただし、電力供給を停止すると、ICカードチップ150の内部状態は、ICカードチップ150内部の不揮発性メモリに記憶されたデータを除いて維持されない。

【0048】CLK2端子153は、ICカードチップ150にクロック信号を入力する端子である。CLK2制御回路127は、CLK2端子153にクロックを供給する回路である。CLK2制御回路127は、CLK0発振器124から供給されたクロック信号をもとにしてCLK2端子153に供給するクロック信号を生成する。CLK2制御回路127はCPU121と接続されており、CLK2端子153へのクロックの供給開始と供給停止をCPU121から制御することができる。ICカードチップ150は、自身内部に駆動クロック発振器をもたない。そのため、CLK2端子153から駆動クロックを供給することによって動作する。CLK2制御回路127が、CLK2端子153へのクロック供給を停止すると、ICカードチップ150の動作は停止するため、ICカードチップ150の消費電力を低下させることができる。この時、VCC2端子151への電力供給が保たれていれば、ICカードチップ150の内部状態は維持される。ここで、CLK2端子153に供給するクロック信号の周波数をF2、CLK0発振器124から供給されたクロック信号の周波数をF0、PとQを正の整数とすると、CLK2制御回路127は、 $F2 = (P/Q) * F0$ の関係になるようなクロック信号を作成して、これをCLK2端子153に供給する。PとQの値はCPU121により設定できるようになってい

る。Pを大きく設定してF2を大きくすると、ICカードチップ150の内部処理をより高速に駆動できる。Qを大きく設定してF2を小さくすると、ICカードチップ150の内部処理はより低速に駆動され、ICカードチップ150の消費電力を低下させることができる。ICカードチップ150の駆動クロック周波数は、ICカードチップ150が正しく動作できるような許容周波数範囲内に設定される必要がある。そのため、CLK2制御回路127は、F2の値がその許容周波数範囲を外れるようなPとQの値を設定させない特徴を持つ。

【0049】I/O端子157は、ICカードチップ150にICカードコマンドを入力したり、ICカードチップ150がICカードレスポンスを出力するときに使用する入出力端子である。ICカードI/F制御回路128は、I/O端子157と接続されており、I/O端子157を通してICカードコマンドの信号送信やICカードレスポンスの信号受信をおこなう回路である。ICカードI/F制御回路128はCPU121に接続されており、CPU121は、ICカードI/F制御回路128によるICカードコマンドやICカードレスポンスの送受信の手続きを制御したり、送信すべきICカードコマンドデータをICカードI/F制御回路128に設定したり、受信したICカードレスポンスをICカードI/F制御回路128から取得する。ICカードI/F制御回路128にはCLK2制御回路127からクロックが供給されており、ICカードコマンドやICカードレスポンスは、CLK2端子153に供給するクロック信号にビット単位で同期して、I/O端子157を通して送受信される。また、RST端子152は、ICカードチップ150をリセットするときにリセット信号を入力する端子である。ICカードI/F制御回路128は、RST端子152と接続されており、CPU121の指示によりICカードチップ150にリセット信号を送ることができる。

【0050】ICカードチップ150は、ICカードの電気信号規格やコマンド規格に基づいて情報交換をおこなう。ICカードチップ150へのアクセスパターンは4種類であり、図3～図6を用いて各パターンを説明する。図3は、CPU121の指示によりICカードチップ150が非活性状態（電源が遮断されている状態）から起動して内部状態を初期化するプロセス（以下、コールドリセットと呼ぶ）において、ICカードチップ150の外部端子の信号波形をシンプルに表したものである。図4は、CPU121の指示によりICカードチップ150が活性状態（電源が供給されている状態）で内部状態を初期化するプロセス（以下、ウォームリセットと呼ぶ）において、ICカードチップ150の外部端子の信号波形をシンプルに表したものである。図5は、CPU121の指示によりICカードチップ150にICカードコマンドを送信しICカードチップ150からI

Cカードレスポンスを受信するプロセスにおいて、ICカードチップ150の外部端子の信号波形をシンプルに表したものである。図6は、CPU121の指示によりICカードチップ150を非活性状態にするプロセスにおいて、ICカードチップ150の外部端子の信号波形をシンプルに表したものである。図3～図6において、時間の方向は左から右にとっており、上の行から下の行に向かってVCC2端子151、RST端子152、CLK2端子153、I/O端子157で観測される信号を表す。また、破線はそれぞれの信号の基準（Lレベル）を表す。

【0051】図3を参照して、ICカードチップ150のコールドリセット操作を説明する。まず、ICカードI/F制御回路128はRST端子152をLレベルにする（301）。次に、VCC2制御回路126はVCC2端子への電源供給を開始する（302）。次に、CLK2制御回路127はCLK2端子153へのクロック信号の供給を開始する（303）。次に、ICカードI/F制御回路128はI/O端子157を状態Z（ブルアップされた状態）にする（304）。次に、ICカードI/F制御回路128はRST端子152をHレベルにする（305）。次に、ICカードI/F制御回路128はI/O端子157から出力されるリセット応答の受信を開始する（306）。リセット応答の受信が終了したら、CLK2制御回路127はCLK2端子153へのクロック信号の供給を停止する（307）。これで、コールドリセットの操作が完了する。なお、ステップ307は消費電力を低下させるための工夫であり、省略してもよい。

【0052】図4を参照して、ICカードチップ150のウォームリセット操作を説明する。まず、CLK2制御回路127はCLK2端子153へのクロック信号の供給を開始する（401）。次に、ICカードI/F制御回路128はRST端子152をLレベルにする（402）。次に、ICカードI/F制御回路128はI/O端子157を状態Zにする（403）。次に、ICカードI/F制御回路128はRST端子152をHレベルにする（404）。次に、ICカードI/F制御回路128はI/O端子157から出力されるリセット応答の受信を開始する（405）。リセット応答の受信が終了したら、CLK2制御回路127はCLK2端子153へのクロック信号の供給を停止する（406）。これで、ウォームリセットの操作が完了する。なお、ステップ406は消費電力を低下させるための工夫であり、省略してもよい。

【0053】図5を参照して、ICカードチップ150にICカードコマンドを送信しICカードチップ150からICカードレスポンスを受信する操作を説明する。まず、CLK2制御回路127はCLK2端子153へのクロック信号の供給を開始する（501）。なお、ク

ロックがすでに供給されている場合、ステップ501は不要である。次に、ICカードI/F制御回路128はI/O端子157にコマンドデータの送信を開始する(502)。コマンドデータの送信が終了したら、ICカードI/F制御回路128はI/O端子157を状態Zにする(503)。次に、ICカードI/F制御回路128はI/O端子157から出力されるレスポンスデータの受信を開始する(504)。レスポンスデータの受信が終了したら、CLK2制御回路127はCLK2端子153へのクロック信号の供給を停止する(505)。これで、ICカードコマンド送信とICカードレスポンス受信の操作が完了する。なお、ステップ505は、消費電力を低下させるための工夫であり、省略してもよい。

【0054】図6を参照して、ICカードチップ150を非活性化する操作を説明する。まず、CLK2制御回路127はCLK2端子153をLレベルにする(601)。次に、ICカードI/F制御回路128はRST端子152をLレベルにする(602)。次に、ICカードI/F制御回路128はI/O端子157をLレベルにする(603)。最後に、VCC2制御回路126はVCC2端子への電源供給を停止する(604)。これで、非活性化の操作が完了する。

【0055】ICカードチップ150は、機密データ保護や個人認証などに必要な暗号演算をおこなうセキュリティ処理機能を持つ。ICカードチップ150は、CPU121との間でICカードコマンドやICカードレスポンスの送受信することにより情報交換をおこない、その結果として、計算の結果や記憶されている情報の送、記憶されている情報の変更などをおこなう。CPU121は、ICカードチップ150を利用してセキュリティ処理を実行することができる。MMC110がホスト機器220から特定のメモリカードコマンドを受信すると、CPU121はそれを契機として、VCC2制御回路126を通してICカードチップ150への電源供給を制御したり、またはCLK2制御回路127を通してICカードチップ150へのクロック供給を制御したり、またはICカードI/F制御回路128を通してICカードチップ150にICカードコマンドを送信する。これにより、CPU121は、ICカードチップ150を利用して、ホスト機器220が要求するセキュリティ処理を実行する。CPU121は、特定のメモリカードコマンドの受信を契機に、ICカードチップ150に対する電源供給制御、クロック供給制御、ICカードコマンド送信、ICカードレスポンス受信を複数組み合わせ

て操作することによって、セキュリティ処理を実行してもよい。また、CPU121は、ホスト機器220がMMC110へ電源供給を開始したのを契機として、セキュリティ処理を実行してもよい。セキュリティ処理の結果は、ICカードチップ150が出力するICカードレスポンスをベースにして構成され、MMC110内に保持される。MMC110がホスト機器220から特定のメモリカードコマンドを受信すると、CPU121はそれを契機として、セキュリティ処理の結果をホスト機器220に送信する。

【0056】図7は、ホスト機器220がMMC110にアクセスするときのフローチャートを表したものである。まず、ホスト機器220はMMC110を活性化するためにVCC1端子144に電源供給を開始する(701)。これを契機として、MMC110は、第1次ICカード初期化処理を実行する(702)。第1次ICカード初期化処理の詳細は後述する。次に、ホスト機器220はMMC110を初期化するためにCMD端子142を通してMMC110の初期化コマンドを送信する(703)。この初期化コマンドはMultiMediaCard仕様に準拠したものであり、複数種類ある。ホスト機器220は、MMC110を初期化するために、複数の初期化コマンドを送信する場合がある。MMC110が初期化コマンドを受信すると、MMC110はそれを処理する(704)。これを契機として、MMC110は、第2次ICカード初期化処理を実行する(705)。第2次ICカード初期化処理の詳細は後述する。ホスト機器220は、MMC110の初期化コマンドに対するメモリカードレスポンスを、CMD端子142を通して受信し、そのメモリカードレスポンスの内容からMMC110の初期化が完了したかを判定する。未完了ならば、再び初期化コマンドの送信をおこなう(703)。MMC110の初期化が完了したならば、ホスト機器220は、MultiMediaCard仕様に準拠した標準メモリカードコマンド(フラッシュメモリチップ130へアクセスするためのコマンド)や、上に述べたセキュリティ処理に関連した特定のメモリカードコマンド(ICカードチップ150へアクセスするためのコマンド)の送信を待機する状態に移る(707)。この待機状態では、ホスト機器220は標準メモリカードコマンドを送信することができる(708)。MMC110が標準メモリカードコマンドを受信したら、MMC110はそれを処理する(709)。処理が完了したら、ホスト機器220は、再び待機状態にもどる(707)。

【0057】この待機状態では、ホスト機器220はセキュリティ処理要求ライトコマンドを送信することもできる(710)。セキュリティ処理要求ライトコマンドとは、上に述べたセキュリティ処理に関連した特定のメモリカードコマンドの1種であり、MMC110にセキュリティ処理を実行させるために処理要求を送信するメモリカードコマンドである。MMC110がセキュリティ処理要求ライトコマンドを受信したら、CPU121は、要求されたセキュリティ処理の内容を解釈し、セキュリティ処理をICカードコマンドの形式で記述する

(711)。即ち、CPU121は、予め定められたルールに従って、ホスト機器230からの標準メモリカードコマンドを、ICカードチップ150が解釈可能な特定のメモリカードコマンドへ変換する。そして、その結果として得られたICカードコマンドをICカードチップ150に発行するなどして、要求されたセキュリティ処理を実行する(712)。処理が完了したら、ホスト機器220は、再び待機状態にもどる(707)。この待機状態では、ホスト機器220はセキュリティ処理結果リードコマンドを送信することもできる(713)。セキュリティ処理結果リードコマンドとは、上に述べたセキュリティ処理に関連した特定のメモリカードコマンドの1種であり、MMC110によるセキュリティ処理の実行結果を知るために処理結果を受信するメモリカードコマンドである。MMC110がセキュリティ処理結果リードコマンドを受信したら、CPU121は、ICカードチップ150から受信したICカードレスポンスをベースに、ホスト機器220に送信すべきセキュリティ処理結果を構築する(714)。そして、ホスト機器220は、MMC110からセキュリティ処理結果を受信する。受信が完了したら、ホスト機器220は、再び待機状態にもどる(707)。なお、ステップ714は、ステップ712の中でおこなってもよい。

【0058】図7において、ステップ702およびステップ705で実行する第1次ICカード初期化処理および第2次ICカード初期化処理は、MMC110内でセキュリティ処理を実行するのに備えて、CPU121がICカードチップ150に対してアクセスする処理である。具体的には、ICカードチップ150の活性化や非活性化、ICカードチップ150のリセット、ICカードチップ150の環境設定を行う。環境設定とは、セキュリティ処理を実行するために必要な情報(例えば、使用可能な暗号アルゴリズムの情報、暗号計算に使用する秘密鍵や公開鍵に関する情報、個人認証に使用する認証データに関する情報など)をICカードチップ150から読み出したり、あるいはICカードチップ150に書き込んだりすることを意味する。ICカードチップ150の環境設定は、ICカードチップ150にICカードコマンドをN個(Nは正の整数)発行することによっておこなう。例えば、セッション鍵が3個必要ならば、ICカードコマンドを3回発行し、セッション鍵が2個必要ならば、ICカードコマンドを2回発行する。N個のICカードコマンドは、互いに相違するものであってもよいし、同一のものであってもよい。Nの値は固定されたものではなく、状況によってさまざまな値となる。以下、環境設定で発行するICカードコマンドを、設定コマンドと呼ぶ。また、この環境設定に基づいてセキュリティ処理を実行するICカードコマンドを、以下、セキュリティコマンドと呼ぶ。セキュリティコマンドの例としては、デジタル署名の計算、デジタル署名の検証、メ

ッセージの暗号化、暗号化メッセージの復号、パスワードによる認証などをおこなうコマンドがある。

【0059】CPU121は、ICカードチップ150の環境設定の内容を自由に変更することができる。CPU121は、セキュリティ処理の内容や結果に応じてこれを変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機としてこれを変更してもよい。また、CPU121は、環境設定の内容を示した情報をフラッシュメモリチップ130にライトし、必要なときにフラッシュメモリチップ130からその情報をリードして使用することもできる。この情報は、図21においてICカード環境設定情報2112として示されている。これにより、MMC110が非活性化されてもその情報を保持することができ、MMC110が活性化されるたびにあらためて設定する手間を省くことができる。

【0060】第1次ICカード初期化処理および第2次ICカード初期化処理は、ICカード制御パラメータA、B、Cに設定された値に基づいておこなわれる。また、CPU121は、ステップ712で実行するセキュリティ処理において、ICカード制御パラメータDに設定された値に基づいてICカードチップ150の活性化や非活性化を制御する。

【0061】図8は、ICカード制御パラメータの種類と設定値、それに対応した処理の内容を表している。まず、パラメータAは、MMC110に電源が供給されたときに実行される第1次ICカード初期化処理に関するパラメータである。A=0のときは、CPU121はICカードチップ150にアクセスしない。A=1のときは、CPU121はICカードチップ150をコールドリセットする。A=2のときは、CPU121はICカードチップ150をコールドリセットした後でICカードチップ150の環境設定をおこなう。A=3のときは、CPU121はICカードチップ150をコールドリセットした後でICカードチップ150の環境設定をおこない、最後にICカードチップ150を非活性化する。A=0またはA=3のときは、第1次ICカード初期化処理のあとICカードチップ150が非活性状態となる。A=1またはA=2のときは、第1次ICカード初期化処理のあとICカードチップ150は活性状態となる。

【0062】次に、パラメータBとCは、MMC110がMMC初期化コマンドを処理したときに実行される第2次ICカード初期化処理に関するパラメータである。B=0のときは、CPU121はICカードチップ150にアクセスしない。B=1かつC=1のときは、CPU121はICカードチップ150をリセット(コールドリセットまたはウォームリセット)する。B=1かつC=2のときは、CPU121はICカードチップ150をリセットした後でICカードチップ150の環境設定をおこなう。B=1かつC=3のときは、CPU12

1はICカードチップ150をリセットした後でICカードチップ150の環境設定をおこない、最後にICカードチップ150を非活性化する。B=2かつC=2のときは、CPU121はICカードチップ150の環境設定をおこなう。B=2かつC=3のときは、CPU121はICカードチップ150の環境設定をおこなった後にICカードチップ150を非活性化する。B=3のときは、ICカードチップ150が活性状態ならば、CPU121はICカードチップ150を非活性化する。最後に、パラメータDは、ホスト機器220から要求されたセキュリティ処理を実行したあとに、ICカードチップ150を非活性化するか否かを示すパラメータである。D=0のときは、セキュリティ処理の実行後に、CPU121はICカードチップ150を非活性化せず、活性状態に保つ。D=1のときは、セキュリティ処理の実行後に、CPU121はICカードチップ150を非活性化する。

【0063】CPU121は、ICカード制御パラメータA、B、C、Dの設定値を変更することができる。CPU121は、セキュリティ処理の内容や結果に応じてこれらの設定値を変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機としてこれらの設定値を変更してもよい。また、CPU121は、これらの設定値をフラッシュメモリチップ130にライトし、必要ときにフラッシュメモリチップ130からこれらの設定値をリードして使用することもできる。これらの設定値は、図21においてICカード制御パラメータ211として示されている。これにより、MMC110が非活性化されてもこれらの設定値を保持することができ、MMC110が活性化されるたびにあらためて設定する手間を省くことができる。

【0064】図9は、第1次ICカード初期化処理のフローチャートを表している。初期化処理を開始する(901)と、まず、ICカード制御パラメータAが0かチェックする(902)。A=0ならばそのまま初期化処理は終了する(908)。A=0でないならばICカードチップ150をコールドリセットする(903)。次に、ICカード制御パラメータAが1かチェックする(904)。A=1ならば初期化処理は終了する(908)。A=1でないならばICカードチップ150の環境設定をおこなう(905)。次に、ICカード制御パラメータAが2かチェックする(906)。A=2ならば初期化処理は終了する(908)。A=2でないならばICカードチップ150を非活性化する(907)。そして、初期化処理は終了する(908)。

【0065】図10は、第2次ICカード初期化処理のフローチャートを表している。初期化処理を開始する(1001)と、まず、ICカード制御パラメータBが0かチェックする(1002)。B=0ならばそのまま初期化処理は終了する(1013)。B=0でないなら

ばB=1かチェックする(1003)。B=1ならばICカード制御パラメータAが0または3かチェックする(1004)。Aが0または3ならば、ICカードチップ150をコールドリセットし(1005)、ステップ1007に移る。Aが1または2ならば、ICカードチップ150をウォームリセットし(1006)、ステップ1007に移る。ステップ1007では、ICカード制御パラメータCが1かチェックする。C=1ならば初期化処理は終了する(1013)。C=1でないならばステップ1009に移る。ステップ1003においてB=1でないならば、Bが2かチェックする(1008)。B=2ならばステップ1009に移る。B=2でないならば、ICカード制御パラメータAが0または3かチェックする(1011)。Aが0または3ならば初期化処理を終了する(1013)。Aが1または2ならば、ステップ1012に移る。ステップ1009ではICカードチップ150の環境設定をおこなう。そして、ICカード制御パラメータCが2かチェックする(1010)。C=2ならば初期化処理を終了する(1013)。C=2でないならばステップ1012に移る。ステップ1012ではICカードチップ150を非活性化する。そして、初期化処理を終了する(1013)。

【0066】図11は、ICカードチップ150が非活性状態であるときに第1次ICカード初期化処理あるいは第2次ICカード初期化処理を実行した場合において、ICカードチップ150の外部端子の信号波形をシンプルに表したものである。図12は、ICカードチップ150が活性状態であるときに第2次ICカード初期化処理を実行した場合において、ICカードチップ150の外部端子の信号波形をシンプルに表したものである。図11と図12において、時間の方向は左から右にとっており、上の行から下の行に向かってVCC2端子151、RST端子152、CLK2端子153、I/O端子157で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準(Lレベル)を表す。図11において1102は図3に示したコールドリセットの信号波形を表す。図12において1202は図4に示したウォームリセットの信号波形を表す。図11と図12において、第1設定コマンド処理1104aと1204a、第2設定コマンド処理1104bと1204b、第N設定コマンド処理1104cと1204cは、それぞれ図5に示したICカードコマンド処理の信号波形を表す。ICカードチップ150の環境設定の信号波形1104と1204は、N個の設定コマンド処理の信号波形が連なって構成される。図11と図12において、1106と1206は、それぞれ図6に示した非活性化の信号波形を表す。図11と図12において、縦方向の破線1101、1103、1105、1107、1201、1203、1205、1207はそれぞれ特定の時刻を表す。1101はコールドリセット前の時刻、1201

はウォームリセット前の時刻、1103はコールドリセット後から環境設定前の間にある時刻、1203はウォームリセット後から環境設定前の間にある時刻、1105と1205は環境設定後から非活性化前の間にある時刻、1107と1207は非活性化後の時刻である。

【0067】図11を参照して、第1次ICカード初期化処理実行時の信号波形を示す。ICカード制御パラメータAが0のときは、信号波形に変化はない。A=1のときは、時刻1101から時刻1103までの範囲の信号波形となる。A=2のときは、時刻1101から時刻1105までの範囲の信号波形となる。A=3のときは、時刻1101から時刻1107までの範囲の信号波形となる。

【0068】図11を参照して、ICカード制御パラメータAが0または3のときの、第2次ICカード初期化処理実行時の信号波形を示す。ICカード制御パラメータBが0のときは、信号波形に変化はない。B=1かつICカード制御パラメータC=1のときは、時刻1101から時刻1103までの範囲の信号波形となる。B=1かつC=2のときは、時刻1101から時刻1105までの範囲の信号波形となる。B=1かつC=3のときは、時刻1101から時刻1107までの範囲の信号波形となる。

【0069】図12を参照して、ICカード制御パラメータAが1または2のときの、第2次ICカード初期化処理実行時の信号波形を示す。ICカード制御パラメータBが0のときは、信号波形に変化はない。B=1かつICカード制御パラメータC=1のときは、時刻1201から時刻1203までの範囲の信号波形となる。B=1かつC=2のときは、時刻1201から時刻1205までの範囲の信号波形となる。B=1かつC=3のときは、時刻1201から時刻1207までの範囲の信号波形となる。B=2かつC=2のときは、時刻1203から時刻1205までの範囲の信号波形となる。B=2かつC=3のときは、時刻1203から時刻1207までの範囲の信号波形となる。B=3のときは、時刻1205から時刻1207までの範囲の信号波形となる。

【0070】図13は、図7のステップ712において、CPU121が、ホスト機器220が要求したセキュリティ処理をICカードチップ150によって実行するときのフローチャートを表している。セキュリティ処理を開始する(1301)と、まずICカードチップ150が非活性状態かをチェックする(1302)。非活性状態ならば、ICカードチップ150をコールドリセットし(1303)、ステップ1306に移る。活性状態ならば、ステップ1304に移る。ステップ1304では、ICカードチップ150にICカードコマンドを発行する前にICカードチップ150を再リセットする必要があるかをチェックする。必要があるならば、ICカードチップ150をウォームリセットし(130

5)、ステップ1306に移る。必要がないならば、ステップ1306に移る。ステップ1306では、ICカードチップ150の環境設定をおこなう必要があるかをチェックする。必要があるならば、ICカードチップ150の環境設定をおこない(1307)、ステップ1308に移る。必要がないならば、ステップ1308に移る。ステップ1308では、ICカードチップ150のCLK2端子に供給するクロック信号の周波数F2を設定する。そして、CPU121はICカードチップ150にセキュリティコマンドを発行し、ICカードチップ150はそれを処理する(1309)。セキュリティコマンドの処理時間は、クロック周波数F2に依存する。

【0071】次に、ICカードチップ150が出力するICカードレスポンスにより、その処理が成功したかどうかを判定する(1310)。成功ならば、ステップ1311に移る。失敗ならば、ステップ1312に移る。ステップ1311では、ICカードチップ150に発行すべきセキュリティコマンドが全て完了したかをチェックする。発行すべきセキュリティコマンドがまだあるならば、ステップ1304に移る。発行すべきセキュリティコマンドが全て完了したならば、ステップ1314に移る。ステップ1312では、失敗したセキュリティコマンドをリトライすることが可能かを判定する。リトライできるなら、リトライ設定をおこない(1313)、ステップ1304に移る。リトライ設定とは、リトライすべきセキュリティコマンドやその関連データをCPU121が再度準備することである。リトライできないならステップ1314に移る。これは、ホスト機器220が要求したセキュリティ処理が失敗したことを意味する。ステップ1314では、ICカード制御パラメータDをチェックする。D=1ならば、ICカードチップ150を非活性化して(1315)、セキュリティ処理を終了する(1316)。D=1でないならば、ICカードチップ150を活性状態に保ったままセキュリティ処理を終了する(1316)。図13のフローチャートにおいては、クロック周波数F2を、ステップ1309で発行するセキュリティコマンドの種類によって変えることができるように、ステップ1308をステップ1309の直前に位置させたが、ステップ1308はそれ以外の位置にあってもよい。

【0072】従来のICカードへの攻撃法を有効にしている要因のひとつとして、ICカードの駆動クロックが外部の接続装置から直接供給されることがあげられる。駆動クロックが接続装置の制御下にあるため、タイミング解析や電力差分解析においては、電気信号の測定においてICカード内部処理のタイミングの獲得が容易になる。一方、故障利用解析においては、異常な駆動クロックの供給による演算エラーの発生が容易になる。これに対し、本発明によれば、MMC110内部でICカードチップ150によりセキュリティ処理を実行するとき、

ホスト機器220はICカードチップ150の駆動クロックを直接供給できない。CPU121は、ICカードチップ150へ供給するクロックの周波数F2を自由に設定することができる。これにより、ホスト機器220の要求する処理性能に柔軟に対応したセキュリティ処理が実現できる。ホスト機器220が高速なセキュリティ処理を要求するならば周波数F2を高く設定し、低い消費電力を要求するならば周波数F2を低く設定したり、クロックを適度に停止させればよい。

【0073】また、CPU121は、周波数F2だけでなくクロックの供給開始タイミング、供給停止タイミングを自由に設定できる。これらをランダムに変化させることにより、ICカードチップ150に対するタイミング解析、電力差分析、故障利用解析と呼ばれる攻撃法を困難にすることができる。タイミング解析は、攻撃者が暗号処理1回の処理時間を正確に計測可能であることを仮定しているため、その対策としては、攻撃者が処理時間計測を正確に行えないようにすることが有効である。本発明によりタイミング解析が困難になる理由は、ICカードチップ150がICカードコマンドを処理している時間の長さをホスト機器220が正確に計測できないためである。電力差分析の対策としては、処理の実行タイミングや順序に関する情報を外部から検出不可能にすることが有効である。本発明により電力差分析が困難になる理由は、ICカードコマンドが発行された時刻、発行されたICカードコマンドの内容、発行されたICカードコマンドの順序（ICカードコマンドを複数組み合わせさせてセキュリティ処理を実行する場合）の検出がホスト機器220にとって困難になるためである。

【0074】故障利用解析の対策としては、ICカードにクロックや電圧や温度等の動作環境検出回路を搭載し、異常を検出したならば処理を停止あるいは使用不能にするという方法が有効である。本発明により故障利用解析が困難になる理由は、CLK2制御回路127がICカードチップ150に異常な駆動クロックを供給しないことが、ホスト機器220がICカードチップ150に演算エラーを発生させるのを防止するからである。

【0075】CPU121は、ICカードチップ150に供給するクロックの周波数F2、供給開始タイミング、供給停止タイミングの設定値を、セキュリティ処理の内容や結果に応じて変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機として変更してもよい。また、CPU121は、これらの設定値をフラッシュメモリチップ130にライトし、必要なときにフラッシュメモリチップ130からこれらの設定値をリードして使用することもできる。これらの設定値は、図21においてCLK2設定情報2113として示されている。これにより、MMC110が非活性化されてもこれらの設定値を保持することができ、MMC110が活性化されるたびにあらためて設定する手間を省くことがで

きる。

【0076】図14は、ホスト機器220がセキュリティ処理要求ライトコマンドをMMC110に発行してから、ICカードチップ150でセキュリティ処理が実行されるまでの過程（図7のステップ710～712）において、MMC110およびICカードチップ150の外部端子の信号波形、CPU121によるフラッシュメモリチップ130へのアクセスをシンプルに表したものである。図14において、時間の方向は左から右にと

る。

【0077】一番上の行はフラッシュメモリチップ130へのアクセス内容である。上から二行目の行から下の行に向かって、VCC1端子144、CMD端子142、CLK1端子145、DAT端子147、VCC2端子151、RST端子152、CLK2端子153、I/O端子157で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Lレベル）を表す。図14を参照して、ホスト機器220がセキュリティ処理要求ライトコマンドをMMC110に発行してから、ICカードチップ150でセキュリティ処理が実行されるまでの過程を説明する。

【0078】まず、ホスト機器220はCMD端子142にセキュリティ処理要求ライトコマンドを送信する（1401）。次に、ホスト機器220はCMD端子142からセキュリティ処理要求ライトコマンドのレスポンスを受信する（1402）。このレスポンスは、MMC110がコマンドを受信したことをホスト機器220に伝えるものであり、セキュリティ処理の実行結果ではない。次に、ホスト機器220はDAT端子147にセキュリティ処理要求を送信する（1403）。セキュリティ処理要求とは、セキュリティ処理の内容や処理すべきデータを含むホストデータである。次に、MMC110はDAT端子147をLレベルにセットする（1404）。MMC110は、これによりビジー状態であることをホスト機器220に示す。次に、CPU121は、ホスト機器220から受信したセキュリティ処理要求をフラッシュメモリチップ130にライトするコマンドを発行する（1405）。セキュリティ処理要求をフラッシュメモリチップ130にライトすることにより、CPU121がセキュリティ処理要求をICカードコマンド形式で記述する処理（図7のステップ711）において、CPU121内部のワークメモリの消費量を節約できる。これは、セキュリティ処理要求のデータサイズが大きいときに有効である。

【0079】なお、フラッシュメモリチップ130にライトされたセキュリティ処理要求は、図21においてセキュリティ処理バッファ領域2114に格納される。また、ライトコマンド発行1405は必須な操作ではない。ライト処理期間1406は、フラッシュメモリチップ130がセキュリティ処理要求のライト処理を実行し

ている期間を表す。セキュリティ処理1407はICカードチップ150によるセキュリティ処理の信号波形を表す。この信号波形は図13のフローチャートの遷移過程に依存する。セキュリティ処理1407は、ライト処理期間1406とオーバーラップさせることができる。一般にフラッシュメモリチップ130のライト処理期間1406はミリ秒のオーダーであるため、セキュリティ処理1407とオーバーラップさせることは、セキュリティ処理の全体的な処理時間の短縮にとって有効である。

【0080】リード/ライト1408は、セキュリティ処理1407の実行中に、フラッシュメモリチップ130からセキュリティ処理要求をリードしたり、ICカードチップ150が出力した計算結果をフラッシュメモリチップ130にライトするアクセスを示している。このアクセスにより、CPU121内部のワークメモリの消費量を節約できる。これは、セキュリティ処理要求やセキュリティ処理結果のデータサイズが大きいときに有効である。リード/ライト1408は必須ではない。セキュリティ処理1407が完了したら、MMC110はDAT端子147をHレベルにセットする(1409)。MMC110は、これによりセキュリティ処理が完了したことをホスト機器220に示す。

【0081】図15は、図14におけるセキュリティ処理1407の信号波形の一例を表したものである。図15において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ130へのアクセス内容である。上から二行目の行から下の行に向かって、VCC2端子151、RST端子152、CLK2端子153、I/O端子157で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準(Lレベル)を表す。1501は図3に示したコールドリセットの信号波形を表し、1504は図4に示したウォームリセットの信号波形を表し、1502および1505は図11(あるいは図12)に示した環境設定の信号波形を表し、1503および1506および1507は図5に示したICカードコマンド処理の信号波形を表し、1508は図6に示した非活性化の信号波形を表す。ICカードチップ150の外部端子において図15に示した信号波形が観測されるのは、図13のフローチャートが1301、1302、1303、1306、1307、1308、1309、1310、1311、1304、1305、1306、1307、1308、1309、1310、1311、1304、1306、1308、1309、1310、1311、1314、1315、1316の順で遷移するときである。

【0082】図15を参照して、図14のセキュリティ処理1407の実行中におけるCPU121によるフラッシュメモリチップ130へのアクセス(リード/ライト1408)を説明する。このアクセスには、図21におけるセキュリティ処理バッファ領域2114を使用す

る。リード1509、1511、1512は、それぞれ、セキュリティコマンド処理1503、1506、1507においてICカードチップ150に送信するICカードコマンドを構築するために必要なデータを、フラッシュメモリチップ130からリードするアクセスである。ライト1510は、セキュリティコマンド処理1503においてICカードチップ150が出力した計算結果を、フラッシュメモリチップ130にライトするアクセスである。ライト1513は、セキュリティコマンド処理1506および1507においてICカードチップ150が出力した計算結果を、フラッシュメモリチップ130にまとめてライトするアクセスである。リード1509、1511、1512は、それぞれ、セキュリティコマンド処理1503、1506、1507以前のICカードチップ150へのアクセスとオーバーラップさせることができる。ライト1510、1513は、それぞれ、セキュリティコマンド処理1503、1507以後のICカードチップ150へのアクセスとオーバーラップさせることができる。これらのオーバーラップは、セキュリティ処理の全体的な処理時間の短縮にとって有効である。

【0083】さらに、フラッシュメモリチップ130のライト単位が大きい場合は、ライト1513のように複数の計算結果をまとめてライトすることができる。これは、フラッシュメモリチップ130へのライト回数を削減し、フラッシュメモリチップ130の劣化を遅らせる効果がある。なお、ライト1510、1513でフラッシュメモリチップ130にライトする内容は、ICカードチップ150が出力した計算結果そのものに限定されず、図7のステップ715でホスト機器220に返すセキュリティ処理結果またはその一部であってもよい。この場合、図7のステップ714またはその一部は、ステップ712の中で実行されることになる。

【0084】図16は、ホスト機器220がセキュリティ処理結果リードコマンドをMMC110に発行してから、MMC110がセキュリティ処理結果を出力するまでの過程(図7のステップ713~715)において、MMC110の外部端子の信号波形、CPU121によるフラッシュメモリチップ130へのアクセスをシンプルに表したものである。図16において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ130へのアクセス内容である。上から二行目の行から下の行に向かって、VCC1端子144、CMD端子142、CLK1端子145、DAT端子147で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準(Lレベル)を表す。

【0085】図16を参照して、ホスト機器220がセキュリティ処理結果リードコマンドをMMC110に発行してから、MMC110がセキュリティ処理結果を出力するまでの過程を説明する。まず、ホスト機器220



はCMD端子142にセキュリティ処理結果リードコマンドを送信する(1601)。次に、ホスト機器220はCMD端子142からセキュリティ処理結果リードコマンドのレスポンスを受信する(1602)。このレスポンスは、MMC110がコマンドを受信したことをホスト機器220に伝えるものであり、セキュリティ処理結果ではない。次に、MMC110はDAT端子147をLレベルにセットする(1603)。MMC110は、これによりビジー状態であることをホスト機器220に示す。次に、CPU121は、フラッシュメモリチップ130のセキュリティ処理バッファ領域(図21の2114)から、ICカードチップ150が出力した計算結果をリードする(1604)。CPU121は、これをもとにセキュリティ処理結果を構築し、MMC110がDAT端子147にセキュリティ処理結果を出力する(1605)。

【0086】なお、図7のステップ714またはその一部が、ステップ712の中で実行されている場合、ステップ1604ではフラッシュメモリチップ130のセキュリティ処理バッファ領域(図21の2114)からセキュリティ処理結果またはその一部をリードする。なお、フラッシュメモリチップ130のセキュリティ処理バッファ領域(図21の2114)を利用しないでセキュリティ処理結果を構築する場合、ステップ1604は必要ない。

【0087】MMC110の製造者や管理者は、セキュリティシステムのユーザにMMC110を提供する前やそのユーザが所有するMMC110に問題が発生した時に、MMC110に内蔵されたICカードチップ150に様々な初期データを書きこんだり、ICカードチップ150のテストをおこなったりする必要がある。MMC110の製造者や管理者によるこれらの操作の利便性を高めるために、MMC110は、ICカードチップ150の外部端子をMMC外部端子140に割りつけるインタフェース機能を持つ。これにより、図3～図6で示したようなICカードチップ150へのアクセス信号を、MMC外部端子140から直接受信できる。このようなMMC110の動作モードを、MultiMediaCard仕様に準拠した動作モードと区別して、以下、インタフェース直通モードと呼ぶ。

【0088】インタフェース直通モードについて詳細に説明する。図17は、ICカードチップ150の外部端子をMMC外部端子140に割りつけるときの対応関係の一例を表している。この例では、RST端子152をCS端子141に割り付け、GND2端子155をGND1端子143、146に割り付け、VCC2端子151をVCC1端子144に割り付け、CLK2端子153をCLK1端子145に割り付け、I/O端子157をDAT端子147に割り付ける。このとき、CS端子141とCLK1端子145は入力端子、DAT端子1

47は入出力端子として機能する。

【0089】MMC110は、特定のメモリカードコマンドを受信すると、動作モードをインタフェース直通モードへ移したり、インタフェース直通モードからMultiMediaCard仕様に準拠した動作モードに戻ることができる。以下、動作モードをインタフェース直通モードへ移すメモリカードコマンドを直通化コマンド、動作モードをインタフェース直通モードから通常の状態に戻すメモリカードコマンドを復帰コマンドと呼ぶ。図1を参照して、MMC1/F制御回路123は、VCC2制御回路126、CLK2制御回路127、ICカード1/F制御回路128と接続されており、MMC110がホスト機器220から直通化コマンドを受信すると、CPU121の指示により図17で示した端子割り付けをおこなう。MMC110がホスト機器220から復帰コマンドを受信すると、CPU121の指示により図17で示した端子割り付けを解除し、MMC110はMultiMediaCard仕様に準拠した動作モードに戻る。

【0090】インタフェース直通モードでは、ホスト機器220がICカードチップ150に直接アクセスできるため、セキュリティの観点からインタフェース直通モードを利用できるのは限られた者だけに必要がある。そこで、直通化コマンドの発行には、一般のユーザに知られないパスワードの送信を必要とする。正しいパスワードが入力されないとインタフェース直通モードは利用できない。

【0091】図18は、ホスト機器220が、MMC110の動作モードをMultiMediaCard仕様に準拠した動作モードからインタフェース直通モードに移し、ICカードチップ150に直接アクセスし、その後、MMC110の動作モードを再びMultiMediaCard仕様に準拠した動作モードに戻すまでの処理のフローチャートを表している。ホスト機器220は処理を開始し(1801)、まずMMC110に直通化コマンドを発行する(1802)。MMC110は、直通化コマンドで送信されたパスワードが正しいかチェックする(1803)。正しいければステップ1804に移り、間違っていれば処理は終了する(1810)。ステップ1804では、CPU121は、ICカードチップ150をコールドリセットする。そして、図17で示した端子割り付けをおこないインタフェースを直通化する(1805)。この時点から、ホスト機器220はICカードチップ150に直接アクセスする(1806)。ホスト機器220がICカードチップ150への直接アクセスを終了し、MMC110の動作モードを再びMultiMediaCard仕様に準拠した動作モードに戻すときは、MMC110に復帰コマンドを発行する(1807)。すると、CPU121は図17で示した端子割り付けを解除し、MMC110はMultiMedia

diaCard仕様に準拠した動作モードに戻る(1808)。そして、CPU121は、ICカードチップ150を非活性化する(1809)。以上で、処理は終了する(1810)。

【0092】図19は、図18のステップ1801~1806の過程において、MMC110およびICカードチップ150の外部端子の信号波形をシンプルに表したものである。図19において、時間の方向は左から右にとる。上の行から下の行に向かって、VCC1端子144、CMD端子142、CLK1端子145、DAT端子147、VCC2端子151、RST端子152、CLK2端子153、I/O端子157で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準(Lレベル)を表す。1905は、図3のコールドリセットの信号波形を示す。モード移行時刻1906は、動作モードがインタフェース直通モードに移る時刻を表す。

【0093】図19を参照して、ホスト機器220がMMC110の動作モードをMultiMediaCard仕様に準拠した動作モードからインタフェース直通モードに移しICカードチップ150に直接アクセスする過程を説明する。なお、MMC110のVCC1端子144には3V(VCC2端子151の標準電圧)が供給されている。ホスト機器220がCMD端子142に直通化コマンドを入力すると(1901)、CMD端子142から直通化コマンドのレスポンスが出力される(1902)。このレスポンスは、MMC110がコマンドを受信したことをホスト機器220に伝えるものである。次に、ホスト機器220はDAT端子147にパスワードを入力する(1903)。パスワード入力後、MMC110はDAT端子147にLレベルを出力し(1904)、ビジー状態であることをホスト機器220に示す。ビジー状態の間に、CPU121は、ICカードチップ150をコールドリセットする(1905)。そして、モード移行時刻1906において、動作モードをインタフェース直通モードに移す。このときに、DAT端子147はLレベルからハイインピーダンス状態になる。これにより、ホスト機器220はビジー状態の解除を知ることができる。この時点から、ホスト機器220はICカードチップ150に直接アクセスする。例えば、CLK1端子145にクロックを供給すると(1907)、CLK2端子153にそのクロックが供給される(1908)。また、DAT端子147にICカードコマンドを送信すると(1909)、I/O端子157にそのICカードコマンドが送信される(1910)。

【0094】図20は、図18のステップ1807~1810の過程において、MMC110およびICカードチップ150の外部端子の信号波形をシンプルに表したものである。図20において、時間の方向は左から右にとる。上の行から下の行に向かって、VCC1端子14

4、CMD端子142、CLK1端子145、DAT端子147、VCC2端子151、RST端子152、CLK2端子153、I/O端子157で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準

(Lレベル)を表す。モード復帰時刻2003は、動作モードがインタフェース直通モードからMultiMediaCard仕様に準拠した動作モードに戻る時刻を表す。2004は、図6の非活性化の信号波形を示す。

【0095】図20を参照して、ホスト機器220がMMC110の動作モードをインタフェース直通モードからMultiMediaCard仕様に準拠した動作モードに戻す過程を説明する。なお、MMC110のVCC1端子144には3V(VCC2端子151の標準電圧)が供給されている。ホスト機器220がCMD端子142に復帰コマンドを入力すると(2001)、CMD端子142から復帰コマンドのレスポンスが出力される(2002)。このレスポンスは、MMC110がコマンドを受信したことをホスト機器220に伝えるものである。そして、モード復帰時刻2003において、MMC110はDAT端子147にLレベルを出力してビジー状態であることをホスト機器220に示し、それと同時に動作モードをMultiMediaCard仕様に準拠した動作モードに戻る。ビジー状態の間に、CPU121は、ICカードチップ150を非活性化する(2004)。そして、MMC110は、DAT端子147をハイインピーダンス状態にし(2005)、復帰コマンドの処理が完了したことをホスト機器220に示す。これ以後、ホスト機器220はICカードチップ150に直接アクセスできない。ホスト機器220が、CLK1端子145にクロックを供給しながらCMD端子142に何らかのメモリカードコマンドを送信した場合、ICカードチップ150にそのクロック信号(2006)は伝わらない。2001や2002においてホスト機器220がCLK1端子145に供給するクロック信号は、ICカードチップ150のCLK2端子153にも伝わるが、DAT端子147がハイインピーダンス状態であるため、ICカードチップ150がICカードコマンドを誤って認識することはない。

【0096】図21において、セキュリティ処理ステータス領域2116には、ICカードチップ150によるセキュリティ処理の進捗状況を示す情報を格納する。CPU121は、この情報をセキュリティ処理の実行中に更新することができる。例えば、セキュリティ処理の途中でMMC110への電源供給が停止した場合、電源供給再開時にCPU121がこの情報をリードして参照すれば、セキュリティ処理を中断した段階から再開することができる。

【0097】次に、本発明の他の実施形態について説明する。

【0098】図27は、本発明を適用したカード型記憶

装置2701の構成を示した図である。記憶装置2701は、フラッシュメモリチップ130、コントローラチップ120、ICカードチップ150、モード選択回路2710、及びMMC外部端子140を有する。モード選択回路2710は、モード選択信号2720に基づいて、モード選択回路2710に接続された入出力バス2730及び入出力バス2740のうちいずれか一つを選択し、MMC外部端子140とコントローラチップ120、又はMMC外部端子140とICカードチップ150とを論理的に接続する機能を持っている。フラッシュメモリチップ130、コントローラチップ120、ICカードチップ150、及びMMC外部端子140の各々のモジュールは、図22で示したMMC110の各々のモジュールと同等の機能を有する。

【0099】カード型記憶装置2701は、モード選択信号2720の状態に応じて、MMC又はICカードとして動作する。図28は、モード選択回路2710、入出力バス2730、入出力バス2740、及びMMC外部端子140の接続状態を示した図である。モード選択回路2710は、MMC外部端子140の各々の信号線(141、142、143、144、145、146、147)に対応したスイッチ(2711、2712、2713、2714、2715、2716、2717)を持っている。各スイッチは、モード選択信号2720の状態によりコントローラチップ120の入出力バス2730、又は、ICカードチップ150の入出力バス2740のどちらかとMMC外部端子140を接続する。例えば、CS141端子は、コントローラチップ120の入出力バス2730のCS2731か、ICカードチップ150の入出力バス2740のRST152のどちらかに接続される。

【0100】ホスト機器2702は、例えばICカードに対応した端末(携帯電話、携帯情報端末(PDA)、パーソナルコンピュータ、音楽再生(及び録音)装置、カメラ、ビデオカメラ、自動預金預払器(ATM)、セットトップボックス(STB)、街角端末、決済端末等)において、既存のシステムを有効に活用しながらカード型記憶装置2701をサポートすることができる。

【0101】図29は、ICカード及びカード型記憶装置2701に対応したホスト機器2901が有するICカード制御に関連するモジュールの構成を示す図である。ホスト機器2901は、MMCソケット2910、モード検出回路2930、ICカード制御回路2950、VCC2電源2960、CLK2発信器2970、及びICカードスロット2980を有する。尚、ICカードスロット2980は装備していなくても構わない。MMCソケット2910はMMCソケット端子2920を有しており、図28で示したMMC外部端子140と接続される。MMCソケット2910は、モード検出回路2930に対してモード検出信号2940を出力す

る。モード検出回路2930は、モード検出信号2940の状態により、MMCソケット2910に挿入される記憶装置2701が、ICカードとして動作するかどうか判定する。ICカードとして動作する場合、モード検出回路2930は、ICカード制御回路2950、VCC2電源2960、CLK2発信器2970の各信号線と、MMCソケット端子2920の信号線を適切に接続する。ICカードとして動作しない場合、MMCソケット端子2920の信号線は接続されず、ホスト機器2901は記憶装置2701を認識しないか、又は非対応の記憶装置2701が挿入された旨をユーザに通知する等の処理が行われる。

【0102】図30は、記憶装置2701がMMCソケット2910に挿入された場合の一例を示す図である。MMCソケット2910は、スイッチ3010及びスイッチ3020を備えており、モードの検出を行う。記憶装置2701がMMCソケット2910に挿入されると、スイッチ3010によりその旨が検出され、スイッチ3020に伝播される。スイッチ3020は、例えば突起型の形状をしており、スイッチ3010から伝播された信号に応じて、記憶装置2701の側面に押し込まれる。一方、記憶装置2701は、側面に凹みがあり、凹みの位置にスイッチ3020が挿入される。記憶装置2701が有するスイッチ3030は、スイッチ3020の挿入の状態を検出し、モード選択信号2720を生成し、モード選択回路2710に出力する。これは例えば、モード選択信号2720をVCCと接続し論理値1の状態にすること等で実現できる。

【0103】即ち、記憶装置2701がICカードモード対応のホスト機器2901に挿入された場合はICカードモードが選択され、そうでない場合はMMCモードが選択される。ホスト機器2901は、モード判定をスイッチ3020で行い、ホスト機器2901にICカードインタフェースに対応した記憶装置2701が挿入されたことを示すモード検出信号2940を出力する。これは、例えばモード検出信号2940をVCCと接続し論理値1の状態にすること等で実現できる。

【0104】ここで、側面に凹みの無い記憶装置2701をホスト機器2901に挿入すると、スイッチ3020は挿入されない。つまり、側面に凹みの無い記憶装置2701をICカードモードに対応していない記憶装置2701とすれば、スイッチ3010がオンの状態でかつスイッチ3020の状態と対応するモード検出信号2940が出力されない場合は、ICカードモードに対応していない記憶装置2701がホスト機器2901に挿入されていると判断される。したがって、ホスト機器2901は、スイッチ3010の状態と合わせてICカードモード非対応の記憶装置2701が挿入されたと判定する。なお、スイッチ3010並びにスイッチ3020はバネ等を利用した機械的なスイッチでも良いし、電気

的なスイッチでも良い。

【0105】図31は、記憶装置2701における処理手順を示したフローチャートである。記憶装置2701がホスト機器2901に挿入されると（S3101）、記憶装置2701が有するスイッチ3030の状態が決まり（S3102）、モード選択信号2720が確定する（S3103）。その後、電源端子VCC1（144）並びにグランド端子GND1（143、146）が接続され（S3104）、記憶装置2701は、モード選択回路2710を起動してモード判定を行う（S3105）。ICカードモードである場合（S3106）、モード選択回路2710は、MMC外部端子140とICチップ信号線（2740）を接続する（S3108）。MMCモードである場合（S3107）、モード選択回路2710は、MMC外部端子140とコントローラチップ信号線2730を接続する。

【0106】上述の実施形態では、一つの記憶装置2701で、ICカードモードとMMCモードを使い分ける一例を示した。次に、他の実施形態について述べる。

【0107】図32は、上述のICカードモード及びMMCモードをサポートしたカード型記憶装置3210の概観を示す図である。ここでは便宜上、端子が装着されている面をB面3220、その反対面をA面3210とする。通常、ユーザがA面3210とB面3220を間違えて挿入できないように、MMCには、逆挿し防止の機能を有する、挿入方向の片端に斜めの切れ込みが入っている。

【0108】カード型記憶装置3210は、MMCと同様の切れ込み並びにMMC外部端子3230に加え、その反対側（図では右側）にも同様の切れ込み及びICカード端子3240が装備されている。カード型記憶装置3210は、MMCとして使用される場合はMMCの矢印の示す方向（左側）に、ICカードとして使用される場合はICカードの矢印の示す方向（右側）に、各々挿入されることにより両モードに対応することができる。なお、内部回路の構成については図27において、コントローラチップ120の入出力バス2730とMMC外部端子3230を、またICチップの入出力バス2740とICカード端子3240を各々接続すればよい。この場合、モード選択回路2710は無くてもよい。

【0109】図33は、カード型記憶装置3310において、ICカードモードとMMCモードをサポートする、図32とは異なる構成を示した図である。カード型記憶装置3310の形状はMMCと変わらず、挿入方向の片端に斜めの切れ込みが入っている。本図の構成においては、MMC外部端子3230及びICカード端子3240は、各々B面3320、A面3310のカード挿入方向（図中の右側）に配置されている。即ち、MMCとして使用する場合は、通常のMMCと同様の向きに挿入し、ICカードとして使用する場合は、MMCとは逆

の向きに挿入する。

【0110】図34は、ホスト機器が有するカード型記憶装置3210及び3310に対応するMMCソケット2910の一例を示す図である。（a）タイプ3410は、MMCモードのみをサポートしているホスト機器2702に使用する。この場合、図32及び図33で示したカード型記憶装置3210及び3310をICカードとして挿入しようとしても、ソケット側の斜めの切れ込みにより、逆挿し防止の機能が働いてカード型記憶装置3210及び3310を挿入することはできない。（b）タイプ3420は、ICカードモードのみをサポートしているホスト機器2702に使用する。この場合、（a）タイプ3410とは逆に、MMCとして挿入しようとしても、切れ込みにより逆挿し防止の機能が働いてカード型記憶装置3210及び3310を挿入することはできない。（c）タイプ3430は、ICカードモード及びMMCモードの両方をサポートするホスト機器2901に装着する。両モードの判別は、例えば、スイッチ3431を用いて行う。（c）タイプ3430のソケットにカード型記憶装置3210及び3310がMMCとして挿入された場合、カード型記憶装置3210及び3310が有する斜めの切れ込み部分とスイッチ3431の位置が対応し、スイッチ3431は作動しない。一方、カード型記憶装置3210及び3310がICカードとして挿入された場合、カード型記憶装置3210及び3310の斜めの切れ込み部分がスイッチ3431の位置と対応しないため、カード型記憶装置3210及び3310の角部分がスイッチ3431をカード型記憶装置3210及び3310の挿入方向に押し付ける。これにより、スイッチ3431がONとなる。スイッチ3431がONになった場合、MMCソケット2901の（c）タイプ3430は、挿入されたカード型記憶装置3210及び3310がICカードとして動作することを判別し、ホスト機器2702にその旨を伝える。

【0111】上述した実施形態では、カード型記憶装置3210及び3310の挿入によってICカードモードとMMCモードを判別する例を示したが、モードの判別方法は上述の実施形態だけに限らない。

【0112】図35は、カード型記憶装置3501が手動で動作するスイッチ3510を有する例を示して図である。ユーザは、自分の使用目的に応じてスイッチ3510を切り替えることによりICカードモードとMMCモードを使い分ける。なお、図35では、スイッチ3510はカード型記憶装置3501の側面に配置されているが、いずれの面、例えば、正面又は裏面に配置してもよい。

【0113】以上述べたように、本実施形態では、カード型記憶装置においてICカードモードとMMCモードをサポートし、その判別を適切に行うことにより各々のモードの処理を実行することが可能である。更に本発明

は、ICカードモードとMMCモードに限らず、様々な動作モードにおいて適用することができる。

【0114】図36は、2系統のモードをサポートするカード型記憶装置3610の内部構成を示した図である。カード型記憶装置3610は、フラッシュメモリチップ130、コントローラチップA3620、コントローラチップB3630、モード選択回路3640、及び外部端子3670を有する。カード型記憶装置3601の基本要素は、図27に示した内部構成とほぼ変わらない。コントローラチップA3620及びB3630は、様々なインタフェース制御に適用することができる。例えば、コントローラチップA3620及びB3630は、前述のMMCコントローラチップ120（図22）、SDカードコントローラチップ2420（図24）、メモリスティックコントローラチップ2520（図25）に適用することでき、一つのカード型記憶装置で上記複数のメモリカードに対応することが可能となる。

【0115】また、カード型記憶装置3610は、2系統のモードだけでなく、3系統以上のモードにも容易に拡張することができる。その場合、外部端子3670は、カード型記憶装置3610がサポートするインタフェースのうち、そのインタフェースが使用する端子数が最大のもの、又はそれ以上の端子数を有するように構成する。例えば、MMCとSDカードをサポートする場合は9本、MMCとメモリスティックをサポートする場合は10本の端子を備える。

【0116】モードの切り替え及びモードの判別方法には、前述のようにモード選択信号2720を用いる。勿論、前述のインタフェース直通モードの説明（図17、図18、図19、図20）で述べたように、インタフェースモードをメモリカードのコマンドで切り替える方法も適用できる。前述の例で言えば、インタフェース直通モードへ移すメモリカードコマンド（直通化コマンド）が発行されると、コントローラチップB3630で制御されるインタフェースモードに移行し、インタフェース直通モードから通常の状態に戻すメモリカードコマンド（復帰コマンド）が発行されると、コントローラチップA3620で制御されるインタフェースモードに移行するようにする。なお、図36においては、フラッシュメモリチップ130がコントローラA3620と接続されているが、メモリチップ130が必要のないインタフェースがコントローラA3620で制御される場合、メモリチップ130はコントローラA3620と接続されなくてもよい。また、図36において、メモリチップ130はコントローラB3630と接続されていないが、コントローラA3620を経由して、或いは直接接続されていてもよい。更に、図36では、コントローラA3620並びにコントローラB3630が物理的に存在する場合について記載しているが、一つのコントロ

ーラで多種類のインタフェース制御を行い（エミュレーション）、上述のモードの切り替えによってインタフェースモードを切り替えることも可能である。また、異なるインタフェースを切り替えるだけでなく、同一のインタフェースにおいてバージョンごとにインタフェースを切り替えることも可能である。

【0117】本発明の実施形態によれば、メモリカード外部からICチップの駆動クロックを直接供給しないため、ICチップの処理時間を正確に計測できず、また、処理の実行タイミングや順序の検出が困難になる。さらに、異常な駆動クロックを供給することができず、演算エラーを発生させるのが困難になる。したがって、タイミング解析、電力差分解析、故障利用解析攻撃法に対するセキュリティが向上する。

【0118】本発明の実施形態によれば、メモリカード外部からICチップの制御方式を自由に設定できる。例えば、高速処理が要求されるならば、ICチップの駆動クロックの周波数を高くした制御方式を設定し、低消費電力が要求されるならば、ICチップの駆動クロックの周波数を低くしたり、ICチップの駆動クロックを適度に停止させる制御方式を設定することができる。したがって、セキュリティシステムの要求する処理性能に柔軟に対応したセキュリティ処理が実現できる。

【0119】本発明によれば、ICチップによるセキュリティ処理に必要なデータや、ICチップを管理するための情報を、フラッシュメモリに保持することができる。したがって、セキュリティ処理の利便性を向上させることができる。

【0120】本発明の実施形態によれば、MMCの製造者や管理者が、MMC内部のICチップに直接アクセスすることができる。したがって、MMC内部のICチップの初期化やメンテナンスを、従来のICカードと同様な方法で実現できる。

【0121】本発明の実施形態によれば、フラッシュメモリチップを備えたMMCに、セキュリティ機能を追加する場合、セキュリティ評価機関の認証を予め受けたICカードチップ追加搭載することによって、セキュリティ評価機関によるMMCの認証が不要となるため、MMCの開発期間又は製造期間が短縮する。

【0122】本発明の実施形態によれば、1つのカード型記憶装置において、多種類のインタフェースをサポートし、その判別を適切に行うことにより、場合に応じて各々のインタフェースを使い分けことができ、利便性を向上することができる。

【0123】

【発明の効果】本発明によれば、記憶装置のセキュリティを向上するという効果を奏する。

【0124】更に、本発明によれば、記憶装置の使い勝手を向上するという効果を奏する。

【図面の簡単な説明】

【図1】本発明を適用したMMCの内部構成を示す図である。

【図2】本発明を適用したMMCのホスト機器の内部構成、およびホスト機器とMMCとの接続状態を示す図である。

【図3】ICカードチップのコールドリセット時の信号波形を示す図である。

【図4】ICカードチップのウォームリセット時の信号波形を示す図である。

【図5】ICカードチップのICカードコマンド処理時の信号波形を示す図である。

【図6】ICカードチップの非活性化時の信号波形を示す図である。

【図7】ホスト機器によるMMCへのアクセスを示したフローチャートである。

【図8】ICカード制御パラメータとそれに対応するICカードへの処理内容を示す表である。

【図9】ICカードチップに対する第1次ICカード初期化の詳細なフローチャートである。

【図10】ICカードチップに対する第2次ICカード初期化の詳細なフローチャートである。

【図11】非活性状態のICカードチップに対するICカード初期化時の信号波形を示す図である。

【図12】活性状態のICカードチップに対するICカード初期化時の信号波形を示す図である。

【図13】ICカードチップによるセキュリティ処理の詳細なフローチャートである。

【図14】セキュリティ処理要求ライトコマンドを処理するときの信号波形とフラッシュメモリチップアクセスを示す図である。

【図15】ICカードチップによるセキュリティ処理実行時の信号波形とフラッシュメモリチップアクセスの一例を示す図である。

【図16】セキュリティ処理結果リードコマンドを処理するときの信号波形とフラッシュメモリチップアクセスを示す図である。

【図17】インタフェース直通モードにおけるMMC外部端子とICカードチップ外部端子の対応関係を示す図である。

【図18】インタフェース直通モードへ移行する処理とインタフェース直通モードから復帰する処理のフローチャートである。

【図19】インタフェース直通モードへ移行する処理時の信号波形を示す図である。

【図20】インタフェース直通モードから復帰する処理時の信号波形を示す図である。

【図21】フラッシュメモリチップの内部構成を示す図である。

【図22】本発明を適用したMMCの内部構成を簡単に示す図である。

05 【図23】本発明を適用したMMCをコンテンツ配信に応用した例を示す図である。

【図24】本発明を適用したSDカードの内部構成を簡単に示す図である。

10 【図25】本発明を適用したメモリースティックの内部構成を簡単に示す図である。

【図26】本発明のICカードチップの内部構成を示す図である。

【図27】本発明を適用したカード型記憶装置の内部構成を示す図である。

15 【図28】モード選択回路2710を中心とした入出力バスの接続状態を示す図である。

【図29】本発明を適用したホスト機器におけるICカード制御に関連するモジュール構成を示す図である。

20 【図30】本発明を適用したカード型記憶装置及びMMCソケットの一構成例を示す図である。

【図31】記憶装置挿入時の手順を示すフローチャートである。

【図32】本発明を適用したカード型記憶装置の概観を示す図である。

25 【図33】本発明を適用した他のカード型記憶装置の概観を示す図である。

【図34】本発明を適用したMMCソケットの一例を示す図である。

30 【図35】本発明を適用したスイッチの装備例を示す図である。

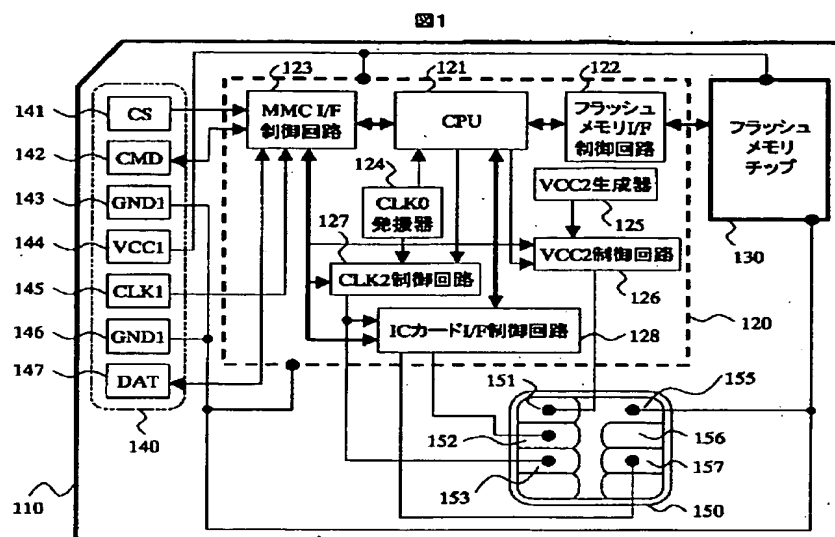
【図36】本発明を適用した他のカード型記憶装置の内部構成を示す図である。

【符号の説明】

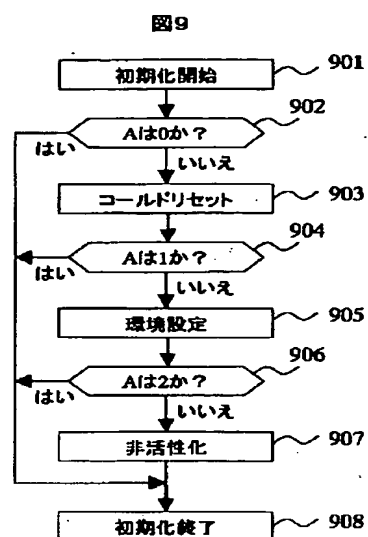
110…MMC、120…コントローラチップ、140…MMC外部端子、150…ICカードチップ、151…VCC2端子、152…RST端子、153…CLK2端子、155…GND2端子、156…VPP端子、157…I/O端子、220…ホスト機器、1405…ライトコマンド発行、1906…モード移行時刻、2003…モード復帰時刻、2701…カード型記憶装置、2710…モード選択回路、2720…モード選択信号、2910…MMCソケット、2930…モード検出回路、2940…モード検出信号、3010…スイッチ、3620…コントローラチップA、3630…コントローラチップB。

35  
40  
45

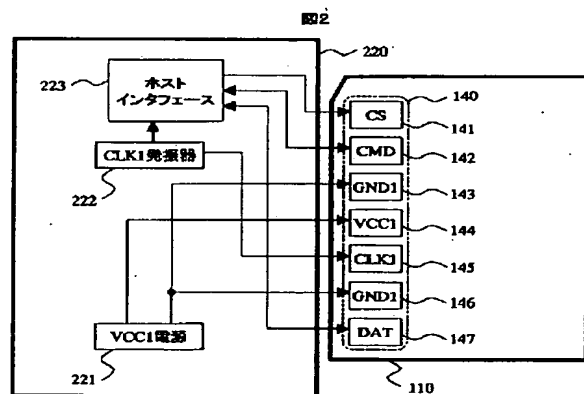
【図1】



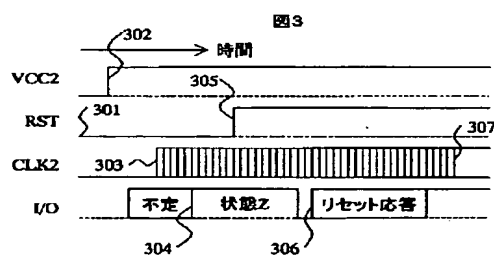
【図9】



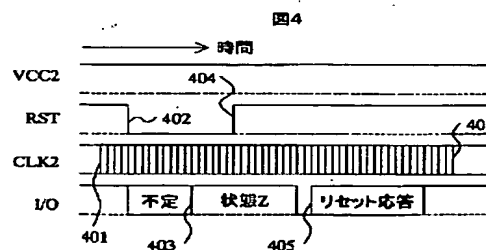
【図2】



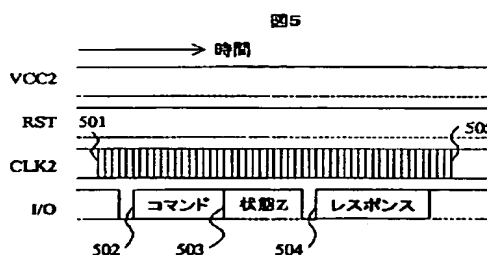
【図3】



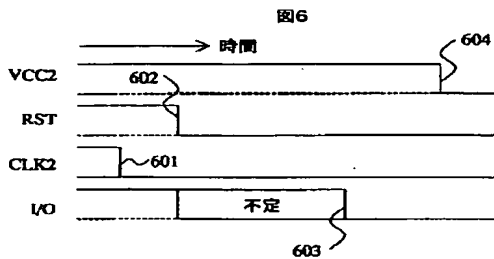
【図4】



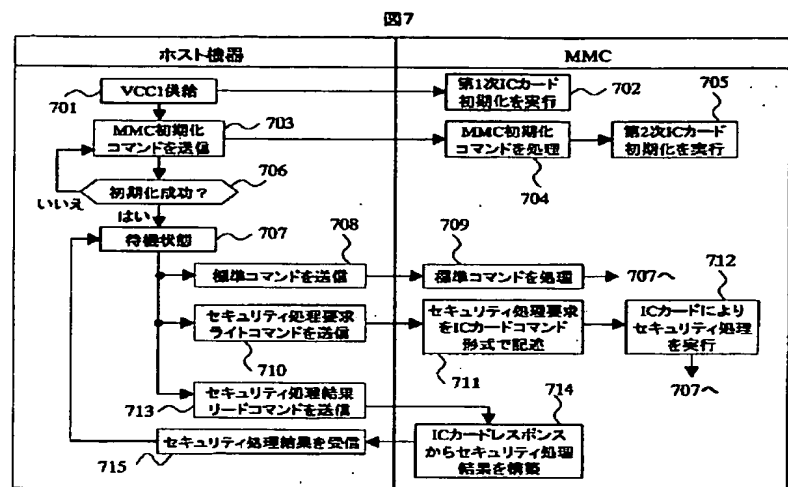
【図5】



【図6】



【図7】



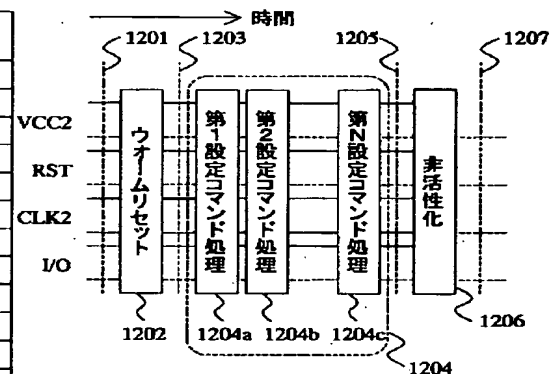
【図8】

図8

ICカード制御パラメータ	ICカードに対する処理
A=0	MMCのパワーオン時に、何もしない
A=1	MMCのパワーオン時に、リセット
A=2	MMCのパワーオン時に、リセットと環境設定
A=3	MMCのパワーオン時に、リセットと環境設定し、非活性化
B=0	MMCの初期化時に、何もしない
B=1	C=1 MMCの初期化時に、リセット
	C=2 MMCの初期化時に、リセットと環境設定
	C=3 MMCの初期化時に、リセットと環境設定し、非活性化
B=2	C=2 MMCの初期化時に、環境設定
	C=3 MMCの初期化時に、環境設定し、非活性化
B=3	MMCの初期化時に、活性状態ならば、非活性化
D=0	セキュリティ処理後に、非活性化しない
D=1	セキュリティ処理後に、非活性化する

【図12】

図12

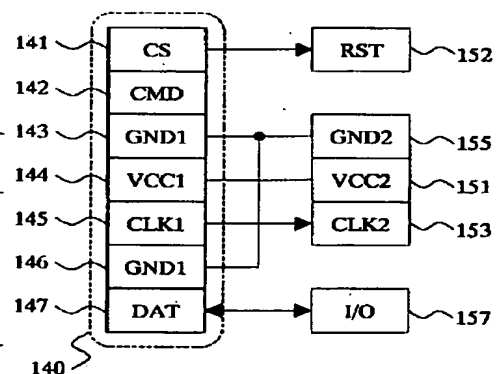
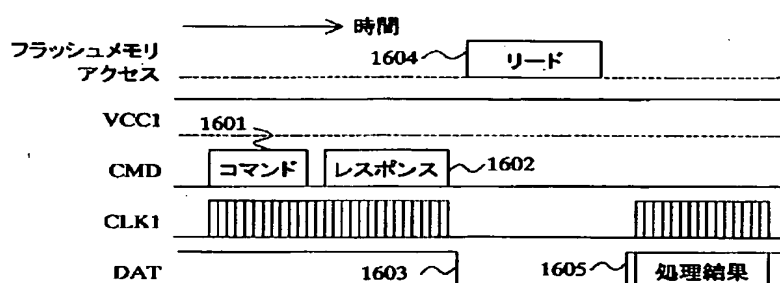


【図17】

図17

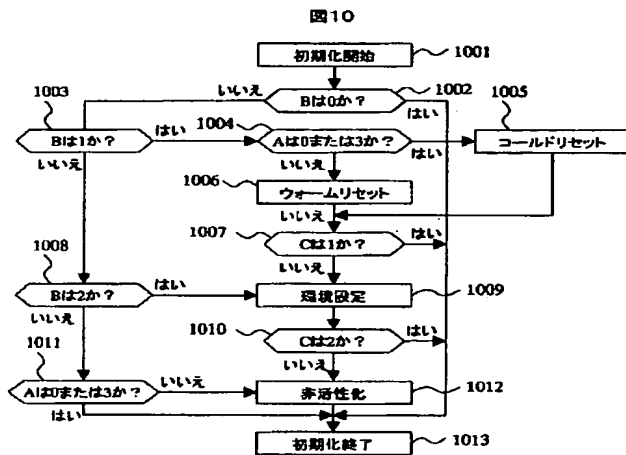
【図16】

図16

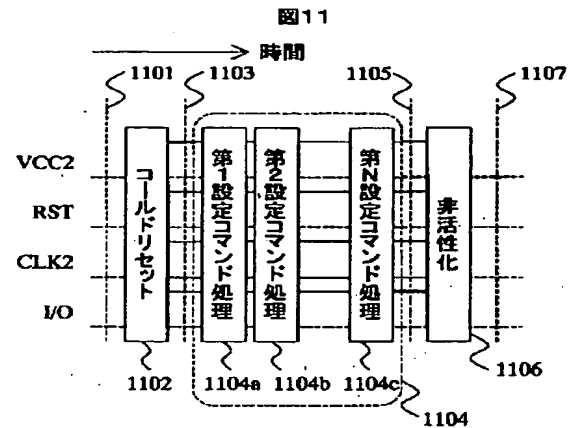




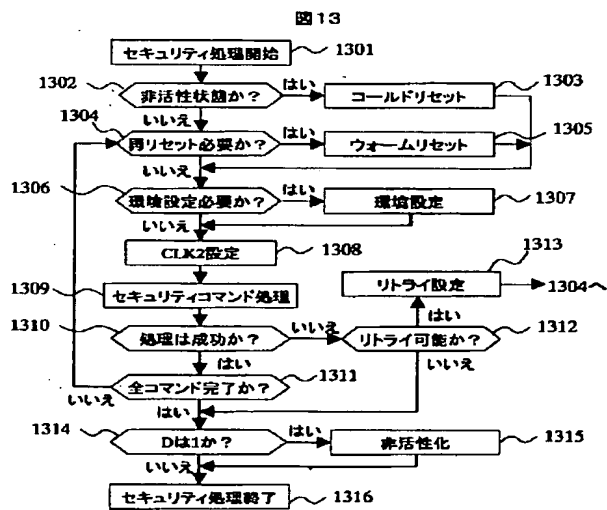
【図10】



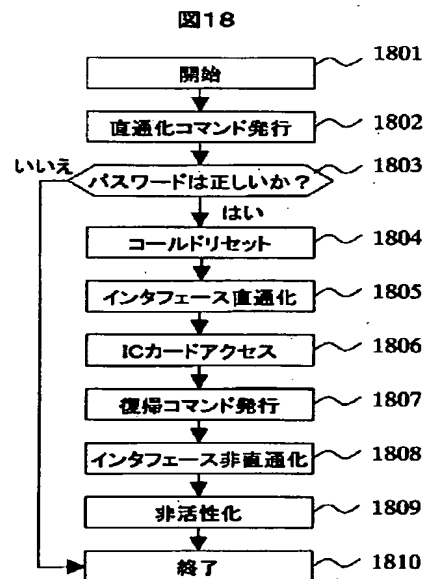
【図11】



【図13】

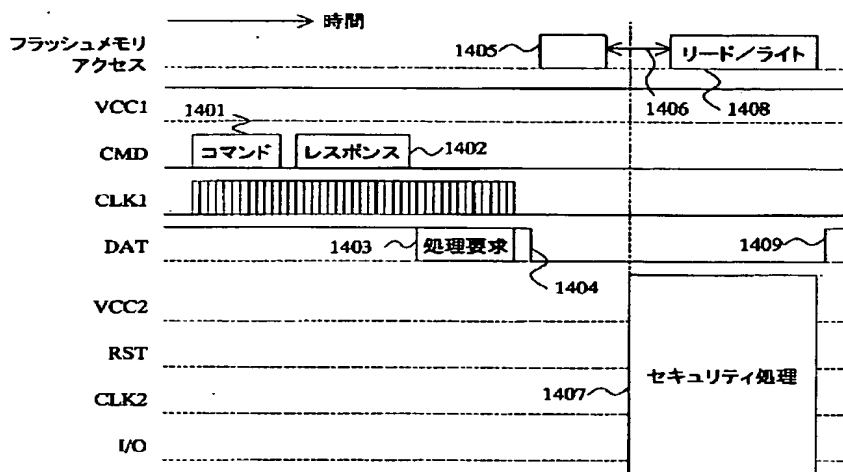


【図18】



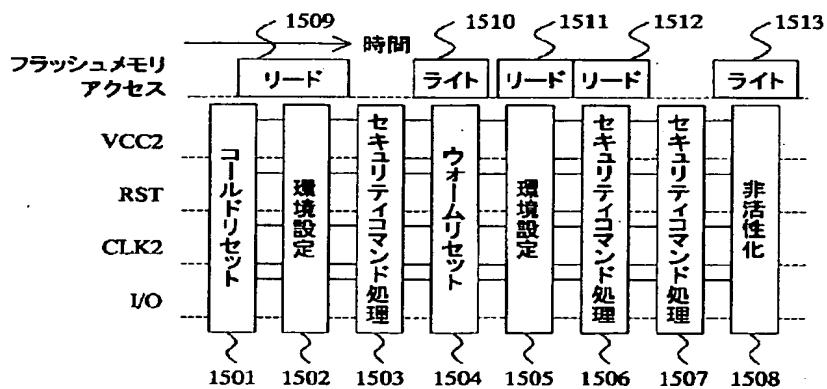
【図14】

図14



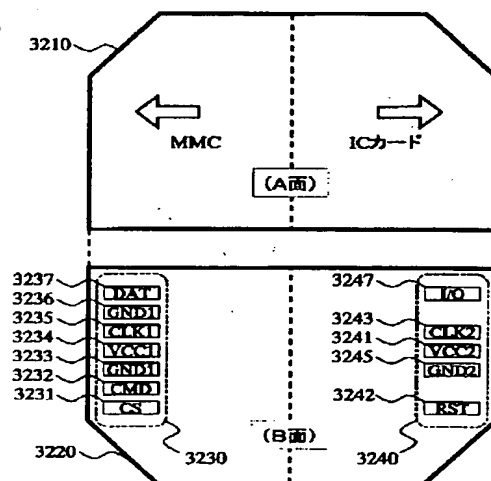
【図15】

図15

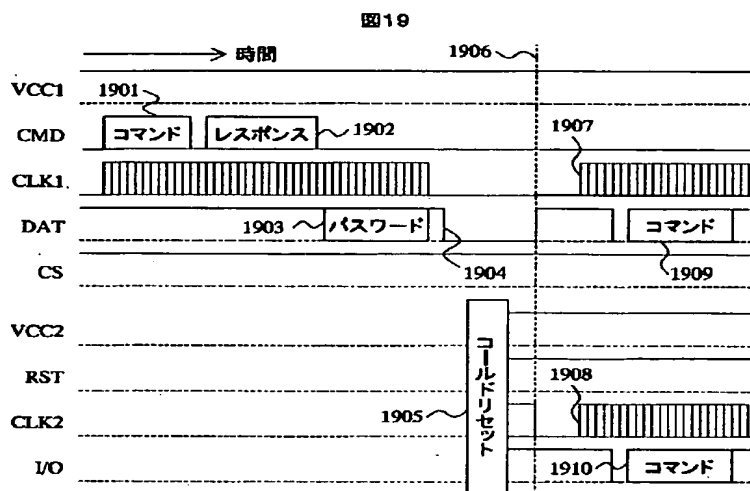


【図32】

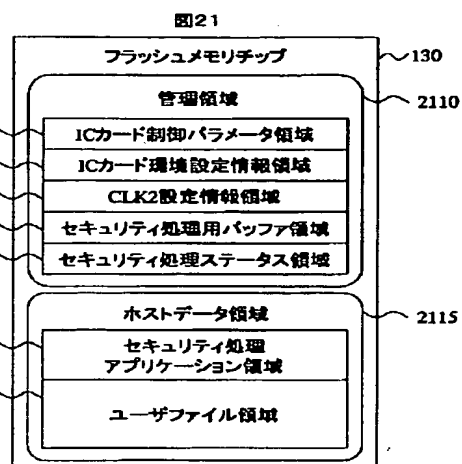
図32



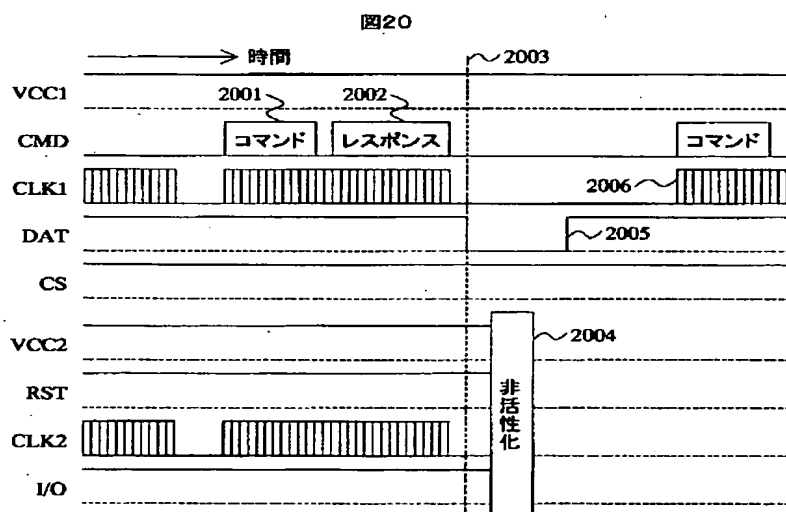
【図19】



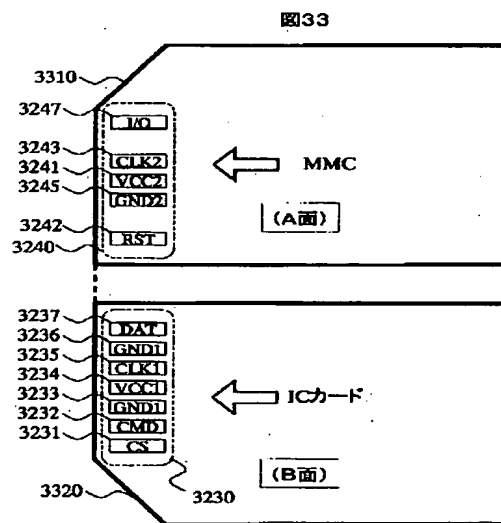
【図21】



【図20】

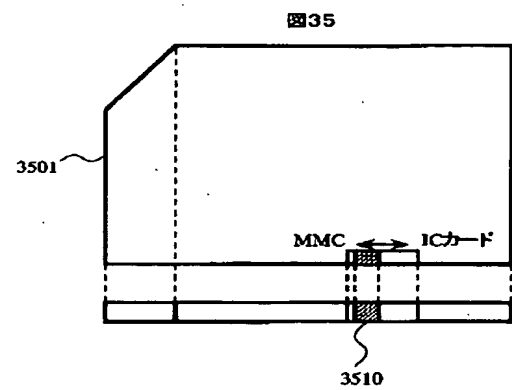
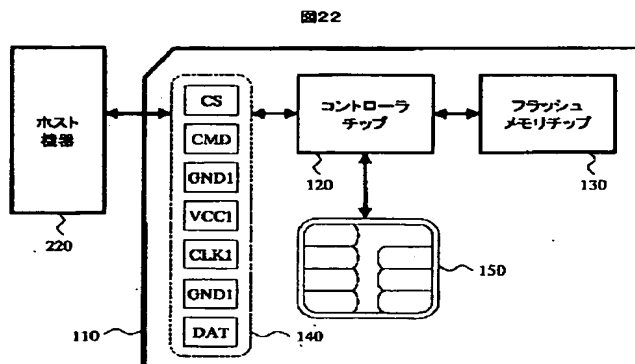


【図33】



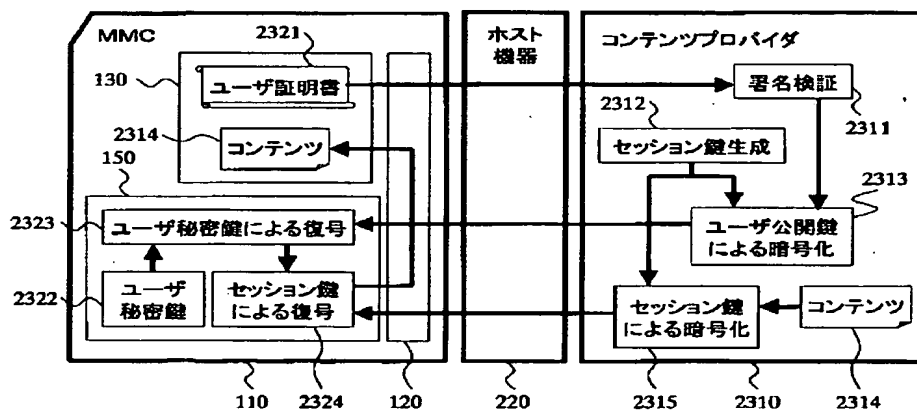
【図 2 2】

【图 3 5】



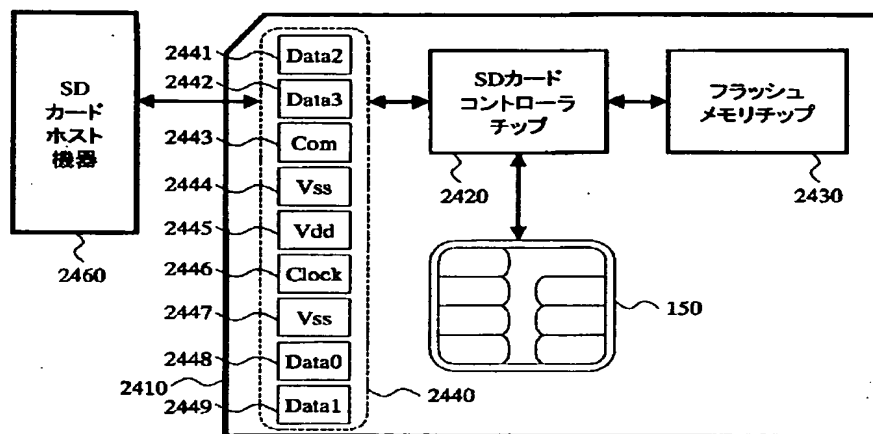
【図 2 3】

**圖23**



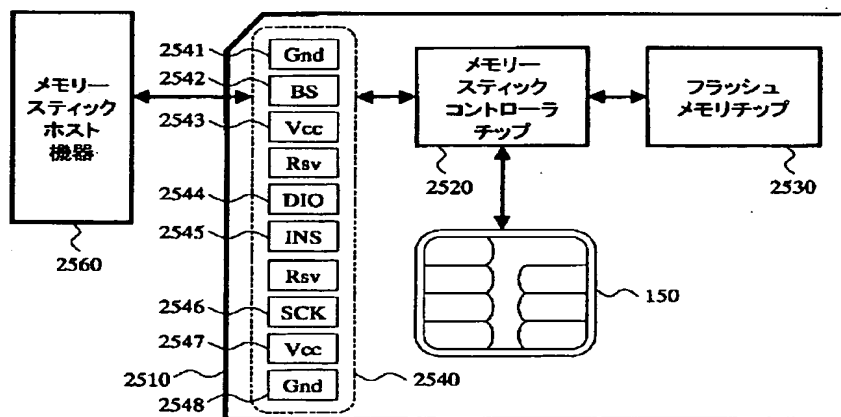
【図24】

図24



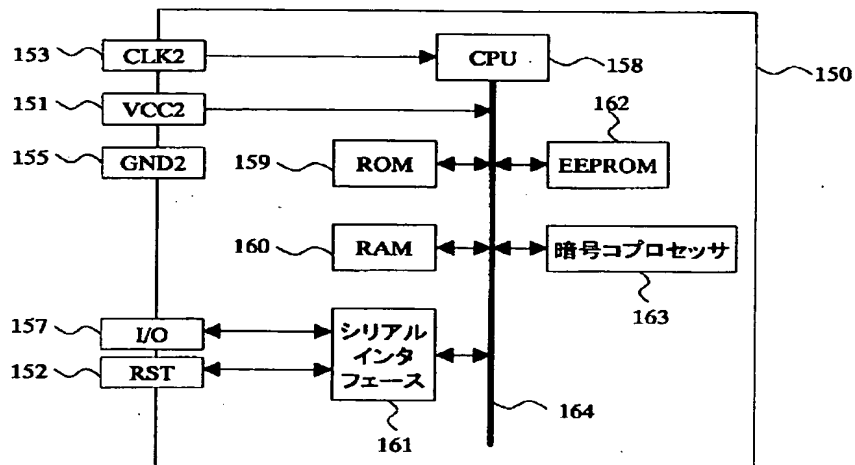
【図25】

図25



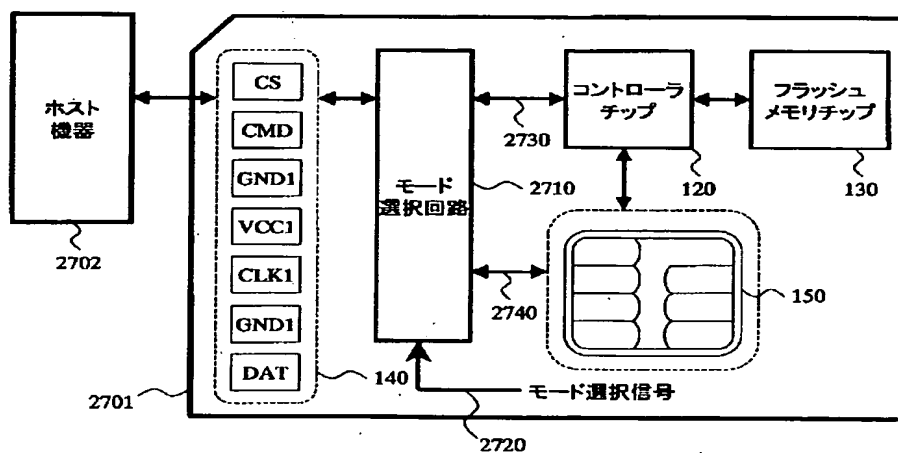
【図26】

図26



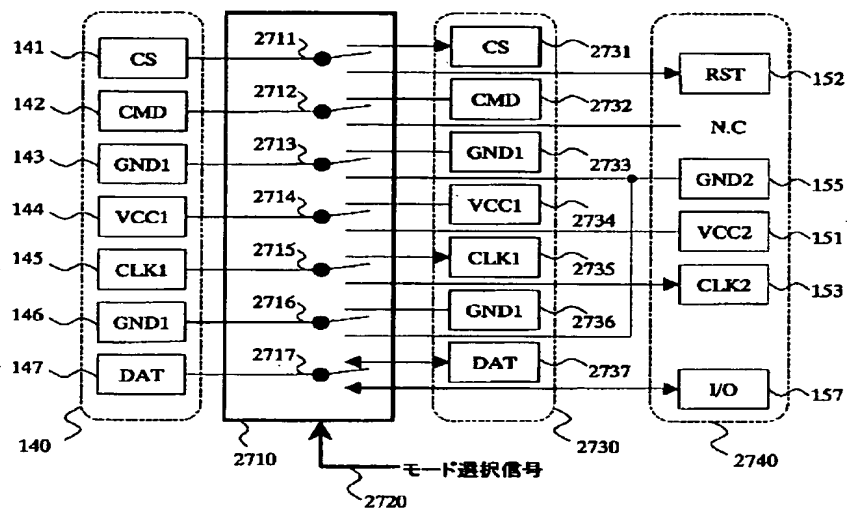
【図27】

図27



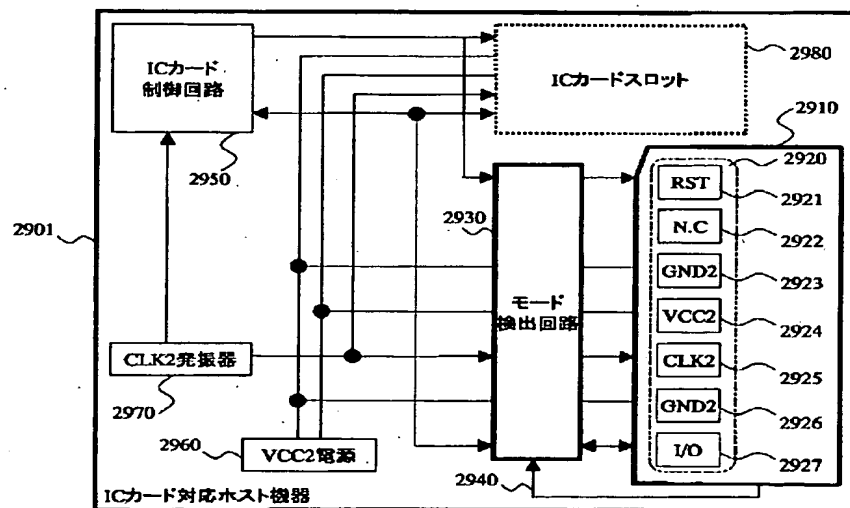
【図 28】

**图28**

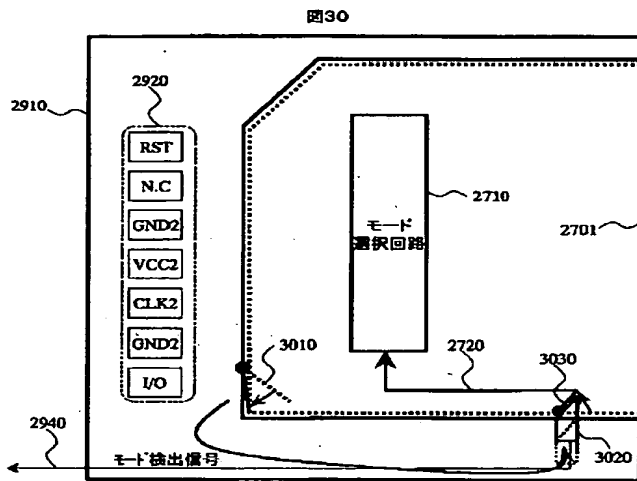


【図 29】

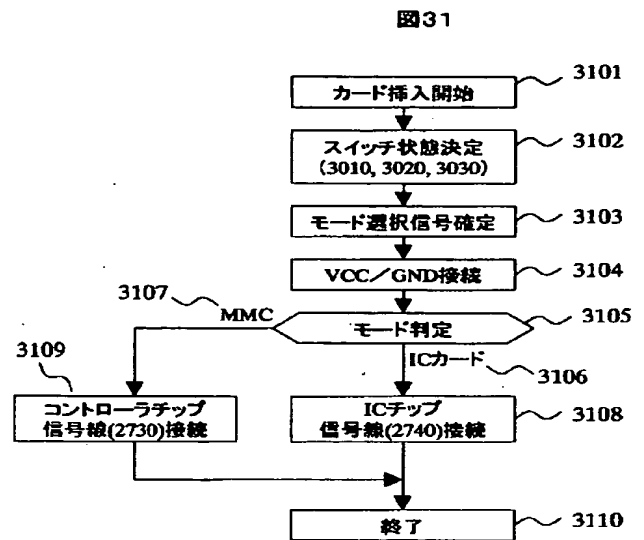
**29**



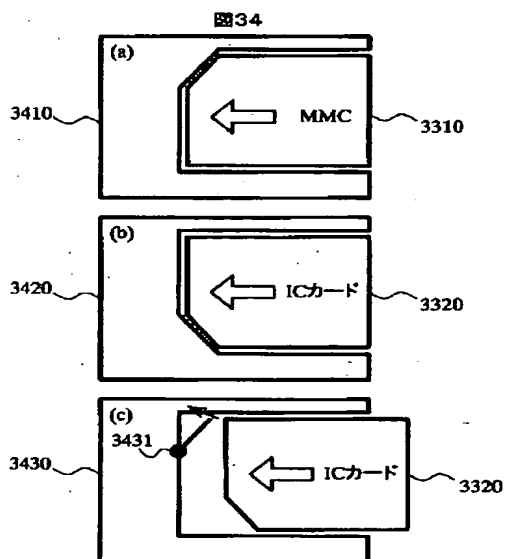
【図30】



【図31】



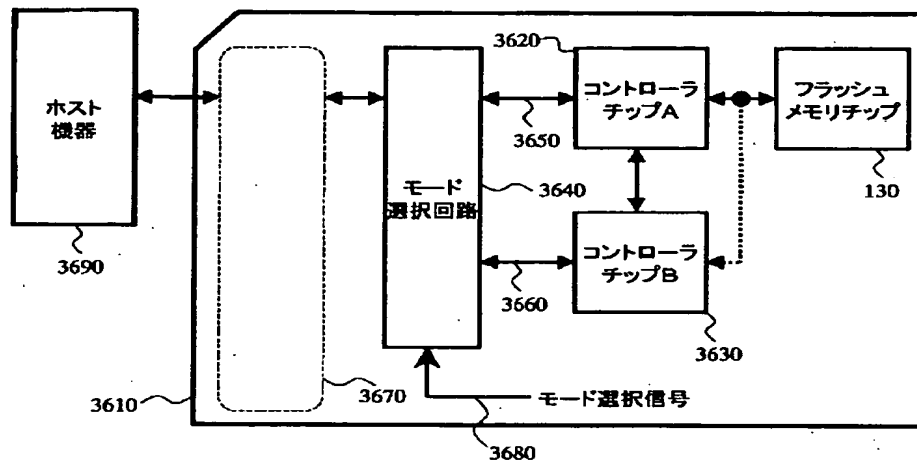
【図34】





【図36】

図36



フロントページの続き

(72) 発明者 片山 国弘

東京都小平市上水本町五丁目20番1号 株  
式会社日立製作所半導体グループ内

25 Fターム(参考) 5B025 AE00 AE10

5B035 AA11 AA13 BB09 CA07 CA11  
CA225B058 CA13 CA23 CA26 CA27 KA02  
KA04 KA21 KA31 YA20

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**